

February 16, 2012

KELLEY DRYE & WARREN LLP
www.kelleydrye.com

**Privacy in 2012:
What to Watch Regarding
COPPA, Mobile Apps, and
Evolving Law Enforcement and
Public Policy Trends**

TABLE OF CONTENTS



- Agenda
- Speaker Bios
- Kelley Drye Privacy & Information Security Practice
- Moderator Bios
- Supplemental Resources

PRIVACY IN 2012

What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends

Presented by Kelley Drye & Warren LLP

February 16, 2012

2:30 – 2:35 PM ET: Welcome

2:35 – 3:00: Keynote

Peter Swire, Professor of Law, Ohio State University; former Clinton Administration Chief Counselor for Privacy, U.S. Office of Management and Budget

3:00 – 4:00: Panel 1

Coping with COPPA: Children's Privacy and Proposed Revisions to the COPPA Rule

Ellen Blackler, Vice President - Global Public Policy, The Walt Disney Company

Mamie Kresses, Senior Attorney, Division of Advertising Practices, Federal Trade Commission

Saira Nayak, Director of Policy, TRUSTe

Moderated by partners **Dana Rosenfeld** and **Alysa Hutnik** of Kelley Drye & Warren LLP

4:00 – 4:15: Break

4:15 – 5:15: Panel 2

Mobile Apps: A Privacy and Consumer Protection Hot Spot

Michael Altschul, Senior Vice President and General Counsel, CTIA

Jessica Rich, Associate Director, Division of Financial Practices, Federal Trade Commission

Jennifer Tatal, Associate General Counsel, Federal Communications Commission

Moderated by partners **John Heitmann** and **Gonzalo Mon** of Kelley Drye & Warren LLP

5:15 – 5:30: Wrap-up discussion

5:30 – 7:00: Cocktail reception

PRIVACY IN 2012

What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends

Presented by Kelley Drye & Warren LLP

Privacy & Information Security Practice

Visit us on the web at www.KelleyDrye.com. For updates on advertising law, privacy, and data security issues and trends, subscribe to our blog, www.AdLawAccess.com. And turn to the www.TelecomLawMonitor.com blog for litigation, enforcement and compliance issue updates.



Dana B. Rosenfeld

Chair, Privacy & Information Security Practice
Partner, Advertising & Marketing Practice

202.342.8588
drosenfeld@kelleydrye.com



John J. Heitmann

Partner
Privacy & Information Security and Telecommunications Practices

202.342.8544
jheitmann@kelleydrye.com



Alysa Z. Hutnik

Partner
Privacy & Information Security and Advertising & Marketing Practices

202.342.8603
ahutnik@kelleydrye.com



Gonzalo E. Mon

Partner
Privacy & Information Security and Advertising & Marketing Practices

202.342.8576
gmon@kelleydrye.com

PRIVACY IN 2012

What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends

Speaker Bios

Peter P. Swire is the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. He is a Senior Fellow with the Center for American Progress and heads a program on encryption and lawful access for the Future of Privacy Forum. From 2009 until August, 2010 Professor Swire was Special Assistant to the President for Economic Policy, serving in the National Economic Council under Lawrence Summers. From 1999 to early 2001 Professor Swire served as the Clinton Administration's Chief Counselor for Privacy, in the U.S. Office of Management and Budget, as the only person to date to have government-wide responsibility for privacy issues. Professor Swire is lead author of *Information Privacy: Official Reference for the Certified Information Privacy Professional*, published by the IAPP. A new edition will be out this year. Many of his writings appear at www.peterswire.net.

Ellen Blackler is Vice President, Global Public Policy at The Walt Disney Company. Ms. Blackler develops public policy positions for The Walt Disney Company on a range of issues related to Internet governance, human rights, privacy and children. Prior to joining Disney, she was on the Public Policy team at AT&T from 2003 to 2011. She previously was Special Assistant to the Chief of the Wireline Competition Bureau at the Federal Communications Commission. Ms. Blackler has also worked at the New York Public Service Commission and the New York State Legislature, where she handled energy and telecommunications issues.

Mamie Kresses is a Senior Attorney with the Division of Advertising Practices at the Federal Trade Commission. She is currently responsible for enforcement of the COPPA Rule and is co-manager of the 2011 COPPA Rule review. In addition to serving as lead counsel in numerous COPPA cases, her work in the areas of online advertising and consumer privacy has included obtaining orders against CyberSpy Software, LLC for unfair marketing of remotely deployed keylogger software, Direct Revenue for deceptive, unauthorized installations of adware, Microsoft for misrepresentations regarding the privacy and security features of "Microsoft Passport," and Eli Lilly for unauthorized disclosure of sensitive personal information. She received the Janet D. Steiger Award for her work as part of the FTC Spyware Team (2006) and the Outstanding Team Award for her work as part of the FTC Privacy Initiative Team (1998).

Saira Nayak is Director of Policy at TRUSTe. In this role, she helps define the company's external policy platform, while advocating the TRUSTe position with industry, regulators, and other stakeholders. Ms. Nayak also counsels TRUSTe clients, as they innovate around today's exciting technologies, while differentiating themselves from the competition with exemplary data collection and use practices. Before TRUSTe, she was Principal at Nayak Strategies, where she advised digital era companies – including TRUSTe - on privacy and data security compliance under international, US and state laws. While in-house at the Microsoft Corporation, Ms. Nayak counseled product groups on privacy and data security compliance, and advised on antitrust compliance matters under Microsoft's consent decree with the US Department of Justice and several state AGs. Before Microsoft, she practiced at Dickstein Shapiro, (Washington, DC), where she advised AT&T, Pfizer, RIAA and other clients on antitrust and consumer protection issues. Ms. Nayak also served as Antitrust Counsel for the National Association of Attorneys General ("NAAG"), where she worked on multistate antitrust investigations and litigation brought by state AG offices.

PRIVACY IN 2012

What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends

Jessica Rich is Associate Director of the Division of Financial Practices within the FTC's Bureau of Consumer Protection. She is a former Deputy Director of the FTC's Bureau of Consumer Protection. Prior to that, Ms. Rich served for 11 years as Assistant and then Associate Director in the FTC's Division of Privacy and Identity Protection. In her various positions, she has overseen a variety of law enforcement and policy matters, including (1) development of FTC rules and regulations, including the COPPA, Gramm-Leach-Bliley Safeguards, FCRA Disposal, and Health Breach Notification Rules (2) law enforcement against companies such as *Microsoft*, *ChoicePoint*, *BJ's Warehouse*, *TJX*, and *LexisNexis* (3) testimony and technical assistance to Congress, and (4) FTC workshops, reports, and policy initiatives, including the Behavioral Advertising Principles and Report, the "Exploring Privacy" roundtable series, and the FTC proposed new privacy framework. Earlier in her career, Ms. Rich served as Legal Advisor to the Director of the FTC's Bureau of Consumer Protection, and was an attorney in privacy practice. Ms. Rich is a graduate of New York University Law School and Harvard College.

Michael Altschul is CTIA's Senior Vice President and General Counsel. He is responsible for the Association's legal advocacy, CTIA's compliance with antitrust and other applicable laws, and he is an active participant in the development of the Association's public policy positions. Mr. Altschul joined CTIA in 1990 after serving with the Antitrust Division of the United States Department of Justice. Prior to that, he began his legal career as an attorney specializing in antitrust litigation with Simpson Thacher Bartlett in New York City. During his ten year stint at the Justice Department, Mr. Altschul worked exclusively on communications matters, including the Modification of Final Judgment and the GTE decree, as well as related FCC filings and telecommunications industry mergers and acquisitions. Mr. Altschul received a Bachelor of Arts in Political Science from Colgate University, and a Juris Doctor from the New York University School of Law.

Jennifer Tatel serves as Associate General Counsel at the Federal Communications Commission. Prior to joining the Office of General Counsel, Ms. Tatel was Legal Advisor for media and consumer issues to Commissioner Meredith Attwell Baker and Chief of the Media Bureau's Industry Analysis Division. Before joining the FCC, she was an attorney at Sidley Austin LLP, working in the firm's Communications and Privacy, Data Security and Information Law practice groups. Prior to attending law school, Ms. Tatel worked as a social worker for the District of Columbia's Child & Family Services Agency. She received her B.S. in Psychology from the University of Illinois, her M.S. in Social Work from Columbia University, and her J.D. from George Washington University Law School.

Privacy and Information Security Practice

Privacy issues are a major focus of Congress, government agencies, state Attorneys General, the media, industry and consumers. The rules are changing rapidly – from looming comprehensive federal legislation; to a patchwork of federal and state laws, regulations and guidance; to expanding industry association requirements and guidelines. Kelley Drye is at the forefront of this evolving area of law. We counsel clients on privacy and security laws governing the collection, use and protection of personal information, and on managing risks and reducing exposure to investigations and litigation arising from how companies handle personal data. We have a national reputation for providing high quality legal services and practical, efficient and timely advice on a broad range of privacy and data security issues. Our team includes several former Federal Trade Commission (FTC) officials and a deep bench of consumer protection law specialists, which uniquely positions us to guide our clients through all aspects involved in privacy and data security matters.

Kelley Drye's Privacy and Information Security practice group helps clients achieve their business goals and a competitive edge while balancing the risks of maintaining customer and employee data. Our attorneys assist clients in designing and updating marketing programs; perform privacy and/or data security compliance and strategic planning and business reviews, including data mapping; draft and amend information security policies and programs; prevent and optimally resolve data breaches; design oversight and monitoring programs for third party handling of customer and employee data; develop and provide privacy training, and represent clients in connection with FTC and state Attorney General investigations and class action litigation. We serve clients in all types of highly-scrutinized industries, including consumer products and retail, hotel and leisure, financial services, and telecommunications, broadband, and technology and mobile services.

Kelley Drye's Privacy and Information Security practice group includes recognized leaders in the field, including two former directors of the FTC's Bureau of Consumer Protection, an Assistant Director, and attorney advisors. While at the FTC, members of our group directed the implementation and enforcement of the Children's Online Privacy Protection Act (COPPA) and the Gramm-Leach Bliley Act (GLBA), and targeted Internet privacy, identity theft, and electronic commerce consumer protection issues. Our group also includes the past chair of the American Bar Association's Privacy and Information Security Committee, former editor-in-chief of the ABA's *Data Security Handbook* and *The Secure Times* newsletter, the co-chairs of the ABA *Consumer Protection Law Developments* treatise, and co-chair of the Federal Communications Bar Association's Privacy and Data Security Committee.

The firm's Privacy and Information Security practice is nationally ranked in *Chambers USA* and *U.S. Legal 500*, and was named one of the top five privacy advisers among law firms and consulting firms around the world in a survey published by *Computerworld* magazine. Notably, sources tell *Chambers* researchers that the group "prioritizes risk to provide practical, thoughtful advice in a timely manner."

This team regularly counsels and represents clients in the following areas:

- **Investigations** – Kelley Drye represents clients in investigations and inquiries from the FTC, state Attorneys General, and other regulatory agencies. We defend clients in federal and state courts and before regulatory agencies regarding their privacy and information security business practices.
- **Compliance and Planning** – We ensure that clients’ business practices are designed to comply with privacy and information security laws, regulations, guidance and applicable industry self-regulatory requirements. We counsel on all aspects of privacy and information security requirements, including the FTC Act, GLBA, COPPA, the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), FCC Customer Proprietary Network Information (CPNI) regulations, the Payment Card Industry Data Security Standard (PCI DSS), Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), state privacy and data security laws, the EU Data Protection Directive and other national and local privacy laws around the world. Our advice also is mindful of the current government enforcement and class action litigation trends on all of these issues.
- **Marketing Campaigns** – Our group counsels clients on how to use consumers’ personal information, geolocation and device data, and CPNI lawfully in marketing, including obtaining effective consent for email marketing, text messaging and online behavioral/preference marketing. We advise clients about their compliance obligations with related laws including the FCC’s CPNI regulations, the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule, and the CAN-SPAM Act. In the early stages of marketing campaigns, the firm represents clients in meetings with privacy advocates to address the use of consumer information, particularly with regard to online and mobile behavior.
- **Policy Development and Training** – Our attorneys help clients draft, review, revise and interpret their privacy, data security and CPNI policies and procedures, and develop appropriate, comprehensive enterprise-wide privacy and data security programs. We also develop and conduct training for clients’ employees on privacy, data security, advertising and business practices that comply with consumer protection laws.
- **Business Practice Audits** – We perform privacy or data security audits of existing business practices. This involves assessing client compliance with current policies and reviewing how clients receive and share personal information and CPNI with affiliates and third parties to ensure that such information sharing complies with laws and business policies, and to ensure that the design of new products and services complies with existing consumer protection law and is balanced with a practical legal risk assessment.
- **Third-Party Compliance** – Kelley Drye helps clients develop and update reasonable oversight and monitoring programs of third party vendors handling consumer data. These efforts, which include developing vendor privacy due diligence templates, drafting and negotiating strategic contractual provisions, and formulating appropriate compliance checks and responses to issues which arise during the relationship, ensure clarity with respect to the parties’ responsibilities and assignment of risk, promote compliance, and reduce exposure in the event a third party vendor mishandles personal data.
- **Data Breach Counseling** – We develop policies and procedures to help clients avoid data breach events and ensure that they are prepared to meet their legal obligations if such an event happens. In the event of a breach, we advise clients on conducting internal and third party investigations as to the source

of the breach, the company's notification obligations, managing public relations, and the overall strategy to reduce the risk of resulting investigations and/or litigation.

- **Litigation** – When a government or industry-based investigation escalates to litigation or a company faces a class action, Kelley Drye's Privacy and Information Security practice has both the subject matter expertise and deep litigation experience needed to develop a robust and cost-effective defense strategy.

As the rules governing privacy and data security change and expand, our Privacy and Information Security lawyers work closely with other members of the firm, including the Advertising and Marketing, Telecommunications, and Government Relations and Public Policy practice groups, to stay ahead of new developments and assist clients in seizing opportunities and protecting against new risks.

Representative Experience

Our attorneys work with clients in a range of industries, including the following areas in which we have extensive expertise:

Technology Providers

Communications and technology providers must be particularly sensitive to privacy and data security issues, given the extensive amount of customer and associated data that they collect. Kelley Drye attorneys help telecom, broadband, mobile, Internet, and other technology providers and related companies understand the myriad laws and regulations which may apply to them, develop policies to remain compliant, and balance the risks associated with holding customer information. The following examples are a representative sampling of the advice our attorneys have provided to clients in this particular area:

- Developed a comprehensive information security program designed to comply with FTC and FCC regulations, as well as state regulations such as the Massachusetts standards, for a major regional integrated communications service provider. This included drafting policies, process documents and training materials, as well as the development of a third party vendor oversight program.
- Provide consumer protection counseling to several major mobile application developers and marketers, including privacy related counseling.
- Provide regular advice to a national retail and carrier on privacy related issues stemming from the FCC's CPNI regulations, the FTC Red Flags rule, COPPA, CAN-SPAM, HIPAA and relevant FTC and state consumer protection, privacy, and data security laws.
- Advised regional fiber provider on vendor certification and contract requests involving GLBA, HIPAA and other privacy-related laws and regulations.
- Provided counseling to a regional broadband provider with respect to responding to law enforcement agency requests, privacy policy revisions, CPNI breach and other breach reporting obligations for services not subject to the FTC Act's common carrier exemption.
- Developed FCC CPNI compliance filings, programs and manuals for a major international carrier.

- Represented telecom and voice over Internet protocol (VoIP) service provider in FCC enforcement proceedings involving CPNI regulation compliance.
- Represented national broadband service provider in FCC rulemaking on CPNI, resulting in rule provisions tailored to carriers serving business customers.
- Developed Red Flags compliance program and training for metropolitan fiber provider.
- Advised cable companies and an applications provider on compliance on with the Cable Act privacy provisions.

Consumer Products and Retail

In the course of marketing and conducting business, retailers are subject to various state and federal laws regulating the collection, use and disclosure of customer information. Violations of such laws and industry standards such as the Payment Card Industry Data Security Standard (PCI-DSS), can result in fines and payment card reimbursement costs often in the six figure range, if not higher. We help companies minimize their risk exposure while meeting their legal and contractual obligations. By way of example, we have addressed the following issues for various clients:

- Assisted a major retailer with a gap analysis for privacy compliance. This involved dividing the business units into discreet parts with similar privacy compliance issues. Our analysis then cataloged every applicable privacy law in the United States (federal and state) in the form of easy-to-follow questions for the business units to answer, which allowed the legal department to identify compliance gaps and most efficiently focus resources on those areas that needed them most.
- Regularly counsel a *Fortune* 50 computer and technology company on global privacy and data security compliance, including assisting on compliance with the various U.S. state developments, enforcement trends and strategies for managing vendor relationships worldwide.
- Appointed Consumer Privacy Ombudsman by United States Trustees in bankruptcy proceedings for three retail companies, submitting reports and recommendations to the courts regarding the disposition of customer lists and other personally identifiable information.
- Assisted major consumer electronics retailers in connection with implementing a behavioral advertising initiative.
- Represented a popular children's specialty retailer in an FTC investigation of the company's in-store and online privacy practices. Successful in convincing the FTC to close the investigation without pursuing law enforcement or remedial action
- Represented a leading academic research company in separate privacy investigations by the FTC and 42 state Attorneys General, and negotiated FTC consent order and state Assurance of Voluntary Compliance.
- Represented an online retailer in investigation of security breaches involving customer information by New York Attorney General's Office, resulting in the negotiation of an Assurance of Discontinuance.
- Represented a leading online retailer in FTC privacy investigation, resulting in the agency's closing of the investigation without further action.

- Provide comprehensive privacy and data security advice for a major online retailer. This includes advising on compliance with COPPA, CAN-SPAM, and relevant FTC and state consumer protection, privacy and data security laws.
- Work with international retailers to review and certify data practices under the Safe Harbor program, to permit them to lawfully transfer its European Union employee and customer data to the United States.

Apparel

Apparel designers, manufacturers and retailers must have the proper privacy and data security compliance programs to ensure customers' personal information is managed appropriately. The following examples are representative of the advice our attorneys have provided to clients in this particular area:

- Counseled a *Fortune* 500 clothing manufacturer on enterprise-wide data security compliance. This included strategies for data protection compliance, legal policies, managing vendor relationships, negotiating privacy and data security terms in vendor contracts, and exercising privacy and due diligence in the company's acquisition of new businesses, data assets and service providers.
- Advised a major clothing and luxury lifestyle retailer on employment-related privacy matters, including disclosures related to the Fair Credit Reporting Act.
- Assisted a luxury brand retailer with designing a program to analyze customer behavior consistent with state and federal privacy laws and concerns.
- Regularly advise *Fortune* 500 and 1000 clothing retailers on privacy and data security matters, including working closely with the companies in designing tailored privacy and data security compliance programs that meet federal and state regulatory requirements.
- Defending an apparel manufacturer in two major California class actions alleging violations of the Song-Beverly Act in the collection of customers' personal information.

Financial Services

Financial institutions face a number of rigorous legal obligations, including compliance with Gramm-Leach-Bliley and the GLB Safeguards Rule. The following examples are representative of the advice our attorneys have provided to clients in this particular area:

- Defended a national financial services company in an FTC investigation for GLBA Safeguards Rule violations. The matter was closed without action.
- Represented a financial institution in an investigation by the FTC concerning an information security breach the business incurred, and whether the company's business practices complied with Section 5 of the FTC Act, the GLBA Safeguards Rule and the GLBA Privacy Rule. The case was resolved with a settlement that included relatively narrow injunctive relief (compared to other similar FTC settlements), and no monetary damages or penalties.
- Counseled numerous clients, including financial service entities, on appropriate responses to a data breach event.

Hotel, Travel and Leisure

Protecting the privacy and security of consumer information can be a challenge for hotels and leisure companies, especially if they have franchises or a decentralized management system. We counsel companies to ensure their privacy and data security policies are uniform across brands and affiliates and advise clients on their obligations in the event of a breach or investigation. The following examples are representative of the advice our attorneys have provided to clients in this particular area:

- Assisted a global, privately-held hospitality and travel company in a data breach situation at one of its hotels involving millions of records containing personally identifiable information.
- Advised a global rental car company on its data breach notification obligations in foreign countries, including the UK, Ireland and Germany.
- Reviewed a video surveillance program and evaluated web camera legal issues in more than 20 countries for one of the world's largest hotel and leisure companies.

Contact Information

For further information about Kelley Drye's Privacy and Information Security practice group please contact **Dana B. Rosenfeld** at (202) 342-8588 or drosenfeld@kelleydrye.com. Visit our blog, www.adlawaccess.com, for updates on advertising law, privacy and information security trends, issues and developments. For further information concerning Kelley Drye & Warren LLP, please visit our website at www.kelleydrye.com.





Dana B. Rosenfeld

PARTNER

WASHINGTON, D.C.

EMAIL: drosenfeld@kelleydrye.com

PHONE: (202) 342-8588

Dana Rosenfeld is a partner in the firm's Washington, D.C. office and chair of the Privacy and Information Security practice. A former assistant director of the Federal Trade Commission (FTC) Bureau of Consumer Protection, Ms. Rosenfeld's practice focuses on all facets of privacy and data security, advertising and consumer financial issues at the federal and state level. She represents clients before the FTC and state Attorneys General – including recent matters for major retailers, food companies, dietary supplement manufacturers, and financial services institutions – and provides ongoing compliance advice related to existing consumer protection laws, best practices and self-regulatory programs.

Ms. Rosenfeld counsels companies in developing and implementing policies on data collection, use and security, consistent with the requirements of the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley Act (GLBA), the Privacy and Safeguards Rules, the Red Flags identity-theft regulations, the FTC Act and corresponding state laws. United States Trustees have recognized her privacy expertise by appointing her Consumer Privacy Ombudsman in the Tower Records, Ritz Camera, and Steve & Barry's bankruptcy proceedings, where she submitted reports and recommendations to the courts regarding the disposition of customer lists and other personally identifiable information.

From August 1998 to October 2001, Ms. Rosenfeld was an assistant director of the FTC's Bureau of Consumer Protection. Prior to this appointment, she was senior legal advisor to the Director of the Bureau of Consumer Protection, and an advisor to FTC Chairman Robert Pitofsky. As assistant director, Ms. Rosenfeld was responsible for coordinating consumer protection policy on advertising and electronic commerce issues.

With a major role in developing the FTC's privacy initiatives, Ms. Rosenfeld helped promulgate the agency's Rules implementing COPPA and GLBA. She also advised the Commission in connection with reports such as the May 2000 Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Marketplace*. Ms. Rosenfeld assisted in the development the FTC's privacy agenda under Chairman Timothy Muris, and chaired the Bureau of Consumer Protection's Internet Legal Issues Task Force effort to apply consumer protection rules and guides to electronic commerce, which focused primarily on the format and presentation of disclosures in Internet advertising.

Ms. Rosenfeld is ranked as a leading practitioner in the Privacy and Data Security area by *Chambers USA*, 2010 and 2011, where clients rave: "She manages projects in a cost-efficient manner that helps us maintain a competitive edge. She is efficient, knowledgeable and has excellent response times – she's a gem!" She is

also mentioned in *US Legal 500* for her work in the Marketing and Advertising and Data Protection and Privacy areas, 2010 and 2011.

Representative Experience

Consumer Protection and Privacy Investigations

Represented the Council of Better Business Bureaus and the Children's Advertising Review Unit of the National Advertising Review Council in developing the Children's Food and Beverage Advertising Initiative, a self-regulatory program designed to encourage the advertising of healthy foods and active lifestyles to children. This project also included the revision of the industry's Self-Regulatory Guidelines for Children's Advertising.

Represented leading children's specialty retailer in an FTC investigation of the company's in-store and online privacy practices. Successful in convincing the FTC to close the investigation without pursuing law enforcement or remedial action.

Represented national toy chain in FTC investigation of the company's gift card practices.

Represented leading academic research company in separate privacy investigations by the FTC and 42 state Attorneys General, and negotiated FTC consent order and state Assurance of Voluntary Compliance.

Represented several companies responding to breaches of data security, including the disclosure of such breaches to consumers and state and federal authorities, as appropriate.

Represented major online retailer in FTC investigation of Mail Order Rule violations, resulting in closing of investigation.

Represented national financial services company in FTC investigation of Gramm-Leach-Bliley Safeguards Rule violations, resulting in closing of investigation.

Represented major telecommunications company in FTC investigation of Fair Credit Reporting Act and Equal Credit Opportunity Act violations, resulting in negotiation of favorable settlement.

Represented online retailer in investigation of security breaches involving customer information by New York Attorney General's Office, resulting in negotiation of Assurance of Discontinuance.

Represented leading online retailer in FTC privacy investigation, resulting in closing of investigation.

Advocacy and Counseling

Regularly counsel companies in developing and implementing privacy policies and data collection and use practices, consistent with the requirements of the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act Privacy and Safeguards Rules, California privacy laws, and FTC and state law enforcement precedent.

Counsel industry associations and individual companies in formulating self-regulatory and corporate social responsibility programs.

Counseled several major consumer products companies in the area of “green” marketing by reviewing advertising claims, developing scientific substantiation, and evaluating potential competitor and law enforcement challenges.

Counseled major entertainment company on roll out of new video on demand service, including review of advertising and marketing materials, customer service policies, and payment systems.

Represented numerous companies seeking FTC support or guidance on consumer protection regulatory issues, legislation or enforcement policy.

Regularly counsel major retailers, including booksellers, jewelers, toy stores, hotel chains and department stores on compliance issues related to state and federal consumer protection laws and regulations.

Assisted clients in various legislative efforts, including preparation of briefing materials, testimony, draft legislation and related materials.

Counseled major real estate management company on all aspects of privacy and data security regulatory compliance, including Fair Credit Reporting Act and Equal Credit Opportunity Act.

Honors and Awards

Selected as one of *The Best Lawyers in America* in the Advertising Law area, 2012.

Ranked as a leading practitioner in the Privacy & Data Security area by *Chambers USA*, 2010 and 2011.

Recommended in *US Legal 500* for her work in the Marketing & Advertising and Data Protection and Privacy areas, 2010 and 2011.

Memberships and Associations

American Bar Association Section on Antitrust, Committee on Consumer Protection and Privacy and Information Security Committee

American Bar Association Committee on Private Advertising Litigation, vice chair

American Bar Association *ANTITRUST* magazine, associate editor

Publications

“The ‘Prior Substantiation’ Doctrine: An Important Check On the Piggyback Class Action,” *Antitrust*, Vol. 26, No. 1, Fall 2011, co-author.

- “Children’s Privacy in the Mobile Data Environment,” *DataGuidance*, October 2011, co-author.
- “Legal Growing Pains In The Mobile App Market,” *The Metropolitan Corporate Counsel*, September 2011, co-author.
- “Data Security Contract Clauses for Service Provider Arrangements,” *Practical Law Company*, July 2011, co-author.
- “Senate Hearing Reflects Increasing Focus on Mobile Privacy and Consumer Protection,” *E-Commerce Law Report*, June 2011, co-author.
- “Defend Against Data Security Risks in Residential Transactions,” *The Title Report*, January 10, 2011, co-author.
- “Can We Say That? A Practical Guide to Substantiating Claims for Food and Consumer Health Products,” *Food and Drug Law Institute Monograph*, Vol 2., No. 3, January 2011, co-author.
- “Congress Explores Consumer Privacy Protection: New Privacy Legislation and FTC Testimony Indicates Direction of Privacy Legislation,” *E-Commerce Law Report*, September 2010, co-author.
- “Data Security and Privacy Audits: Steps to Protect Reports,” *The Secure Times*, June 7, 2010, co-author.
- “Representative Boucher Introduces Privacy Legislation,” *e-Commerce Law Report*, Vol. 12, No. 5, May 2010, co-author.
- “Red Flags Rule Identity Theft Prevention Program Master Policy,” *Practical Law The Journal*, Vol. 2, Issue 3, April 2010, co-author.
- “State Agency Notice Requirements for Data Breaches Chart,” *Practical Law Company*, April 2010, co-author.
- “FTC Warns Companies of Data Leaks on Peer-to-Peer File Sharing Networks,” *Cyberspace Lawyer*, Vol. 15, Issue 2, March 2010, co-author.
- “Federal Trade Commission Continues to Explore Consumer Privacy Protection Measures,” *Privacy & Data Security Law Journal*, Vol. 5, No. 2, February 2010, co-author.
- “Data Security Breach Notice Letter,” *PLC Law Department*, February 2010, co-author.
- “Common Gaps in Information Security Compliance Checklist,” *PLC Law Department*, February 2010, co-author.
- “State Agency Notice Requirements for Data Breaches Chart,” *PLC Law Department*, February 2010, co-author.
- “Nevada and New Hampshire Add Data Security and Privacy Laws,” *Privacy & Data Security Law Journal*, January 2010, co-author.

Speaking Engagements

“Privacy in 2012: What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends,” Kelley Drye Seminar, Washington, D.C., February 16, 2012.

“Understanding The Federal Trade Commission’s Proposed Framework for Consumer Privacy Protection,” The Knowledge Conference Webcast, June 6, 2011.

“Mobile Applications: Privacy and Data Security Considerations,” Kelley Drye Webinar, May 16, 2011.

“A Retailer’s Obligation to Protect Customer and Employee Personally Identifiable Information: A Review of Federal and State Regulatory Requirements, Recent Case Law and Pending Federal Legislation,” DRI Strictly Retail Seminar, Chicago, IL, May 12, 2011.

“Privacy & Information Security Update,” American Bar Association Teleseminar, May 4, 2011.

“Privacy and Data Security in the Cloud,” Vienna, VA, April 29, 2011.

“While Legislation Gets Muddled, Privacy Law Gets Made,” The Future of Privacy Forum, Washington, D.C., April 12, 2011.

“A New Era for the FTC Advertising Substantiation Standards?,” 59th Spring Meeting of the ABA Section of Antitrust Law, Washington, D.C., March 30, 2011.

“A New Decade of Privacy Law Enforcement Policy,” ABA Consumer Protection Conference, Washington, D.C., February 3, 2011.

“Privacy By Design, Choice and Transparency: What a New Framework Will Mean for Business and Technology,” Washington, D.C., January 20, 2011.

“The Revised FTC Green Guides: A Summary from the FTC,” American Bar Association Antitrust Section Teleconference, Washington, D.C., October 12, 2010.

“Dietary Supplements: Federal Enforcement and Consumer Litigation,” ABA Antitrust Section Brown Bag Series, Webinar, September 15, 2010.

“Retail Data Privacy: Top Issues Driving Investigations and Litigation, and How to Avoid Becoming a Target,” General Counsel Roundtable, New York, NY, August 4, 2010.

“Privacy and Data Security Issues Related to Marketing to Minors,” Federal Communications Bar Association Brown Bag Lunch, Washington, D.C., May 19, 2010.

“Privacy and Data Security: Strategies for Avoiding Compliance Gaps, Investigations, and Litigation,” Kelley Drye Continuing Legal Education Seminar, New York, NY, May 5, 2010.

“Security and Privacy in the Cloud: Developing the Right Framework for Service Providers, Business Customers, and Consumers,” American Bar Association Section of Antitrust Law 58th Annual Antitrust Spring Meeting, Washington, D.C., April 23, 2010.

“The FTC’s New Endorsement and Testimonial Guides,” ABA Section of Antitrust Law, Private Advertising Litigation Committee, Washington, DC, December 1, 2009.

“Privacy Law Paradigm Shift: Policymakers Respond to Rapidly Evolving Technologies,” Presented by Kelley Drye, Washington, D.C., November 17, 2009.

Bar Admissions

District of Columbia, 1988

Education

American University Washington College of Law
J.D., 1984

University of Maryland – College Park
B.A., *with honors*, 1981



John J. Heitmann

PARTNER

WASHINGTON, D.C.

EMAIL: jheitmann@kelleydrye.com

PHONE: (202) 342-8544

John Heitmann is a partner in Kelley Drye & Warren LLP's Washington, D.C.-based Telecommunications and Privacy and Information Security practice groups, where he advises broadband and Internet service providers on a broad range of communications law, privacy and data security issues.

Mr. Heitmann has more than fifteen years of experience representing carriers, broadband, Internet and information service providers, Voice over IP (VoIP) providers and other enterprises on regulatory policy, litigation, dispute resolution and enforcement matters before federal and state regulatory agencies, and in state, federal and appellate court litigation. He also counsels extensively on compliance policies and issues arising from the Communications Act, the Federal Trade Commission (FTC) Act, and numerous other federal and state laws governing privacy, information security and telecommunications law issues.

In the broadband and telecommunications arena, Mr. Heitmann has extensive experience in all types of competitive carrier issues such as interconnection, intercarrier compensation, collocation and unbundling. He has extensive experience in regulatory litigation matters and has led numerous carrier coalitions in pursuing public policy decisions favorable to competitive providers' business plans on a wide array of issues including privacy/customer proprietary network information (CPNI) regulation, the federal universal service fund (USF) and merger reviews. He also has negotiated and/or arbitrated interconnection and traffic exchange agreements on behalf of more than a dozen competitive local exchange carriers (CLECs) and multi system operators (MSOs) with dozens of incumbent local exchange carriers (ILECs) and wireless carriers.

In the privacy and information security arena, Mr. Heitmann advises clients on creating public-facing and internal policies and taking actions necessary to achieve compliance with myriad federal and state laws, including the Federal Communications Commission's privacy rules (CPNI), the FTC Act, the Fair Credit Reporting Act, the CAN-SPAM Act, the Telephone Consumer Protection Act, and numerous state data protection and data breach laws and regulations.

Mr. Heitmann also advises clients in transactional matters involving the sale and procurement of telecommunications, broadband capacity, collocation and fiber facilities, and on regulatory issues arising in the context of mergers and acquisitions, product development and strategic planning.

Through the International Association of Privacy Professionals, Mr. Heitmann is a Certified International Privacy Professional (CIPP). He also is co-chair of the Federal Communications Bar Association's (FCBA) Privacy and Data Security Committee and has served as co-chair of the FCBA's State and Local Practice

Committee. Mr. Heitmann was selected as a 2011 Client Service All-Star by BTI Consulting. In 2011, *US Legal 500* recommended Mr. Heitmann for his work in the Telecommunications-Regulatory and Technology, Data Protection and Privacy areas.

Representative Experience

Representing clients in the negotiation and arbitration of interconnection agreements with incumbent landline providers, including rural providers.

Counseling with respect to interconnection and other intercarrier agreement implementation and dispute resolution, including representation in FCC and state enforcement actions.

Defending clients in FCC and other regulatory agency enforcement actions and investigations.

Counseling voice over Internet protocol (VoIP) technology users on regulatory compliance, business strategy and products design.

Representing clients on a wide range of financing, merger and asset transfer transactions, including negotiating intercarrier service arrangements as well as filing applications and securing approvals from the Federal Communications Commission and state public utility commissions.

Representing wireless service providers, landline providers, industry associations and others in rulemaking and other proceedings before the FCC, FTC and state public utility commissions. Areas of expertise include data privacy and security, network neutrality, universal service, unbundled network elements (UNEs), special access, 271 elements, broadband, forbearance, intercarrier compensation, CPNI, mergers, resale and copper loop retirement.

Representing clients in complex interconnection agreement-based litigation and appeals before U.S. Courts of Appeal, federal district courts and multiple state commissions.

Counseling clients on compliance, business strategy, litigation risk, policy development, training and product development with respect to telecom-regulatory and contractual requirements involving a wide array of subject matters, including intercarrier compensation (reciprocal compensation and access charges), UNEs/EELs, collocation, interconnection, building access, provisioning/OSS, privacy/CPNI, universal service/USF, net neutrality, CALEA, pole attachments, truth-in-billing, win-back/retention marketing, slamming, numbering/number portability, 911/E911, regulatory fees, reporting requirements and compliance with law enforcement requests.

Negotiating and drafting telecommunications-related contracts for clients, including mutual traffic exchange agreements with wireless providers, commercial agreements, pole attachment agreements, indefeasible rights of use (IRUs) and backhaul/facility/capacity agreements.

Representing clients in state commission certification and eligible telecommunications carrier (ETC).

Advising clients with respect to and drafting carrier policy statements on Red Flag Rule, acceptable use and network management.

Honors and Awards

Recommended in *US Legal 500* for his work in the Telecommunications-Regulatory and Technology – Data Protection and Privacy areas, 2011.

Selected as a 2011 Client Service All-Star by BTI Consulting.

Memberships and Associations

American Bar Association, Antitrust Section

Federal Communications Bar Association, Co-Chair Privacy and Data Security Committee

Federal Communications Bar Association, Former Co-Chair State and Local Practice Committee

International Association of Privacy Professionals, Certified Information Privacy Professional

Professional Activities

TelecomHUB, Board of Directors

Publications

“Social Media Considerations for US Employers: Analysis,” *Data Protection Law and Policy*, September 2011.

“Groupon Privacy Statement Revisions Reflect Rapid Changes in the Marketplace and an Evolving Legal and Regulatory Landscape,” *NextDailyDeal*, August 18, 2011.

“Avoiding Trouble When Adding an App to the Business Model,” *E-Commerce Law & Policy*, July 2011, co-author.

“The Rise of Mobile Apps: The Privacy Considerations,” *Data Protection Law and Policy*, July 2011, co-author.

“Senate Hearing Reflects Increasing Focus on Mobile Privacy and Consumer Protection,” *E-Commerce Law Report*, June 2011, co-author.

“Time For Broadband Service Providers To Take Note Of Developing Privacy Regulation,” *The Metropolitan Corporate Counsel*, September 2010.

“Federal Communications Commission Proposes “Network Neutrality” Rules Intended to Preserve a Free and Open Internet,” *The Metropolitan Corporate Counsel*, January 2010.

Speaking Engagements

[“Privacy Primer: What Carriers and Service Providers Need to Know Now About Data Privacy and Security,” COMPTEL PLUS Spring 2012 Convention & Expo, San Francisco, CA, April 16, 2012.](#)

[“What Does the Push for Broadband Mean for the Public Switched Network?” Law Seminars International: Telecommunications Law, Seattle, WA, April 12, 2012.](#)

“Smart Privacy Choices for Mobile Apps,” 7th Annual FCBA Privacy & Data Security Symposium, Washington, D.C., March 21, 2012.

[“Take Two – Employees, Smart Phones and Social Media: Best Practices for Mobile Computing and Social Media Policies, IAPP Global Privacy Summit, Washington, D.C., March 8, 2012.](#)

“Privacy in 2012: What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends,” Kelley Drye Seminar, Washington, D.C., February 16, 2012.

[“Wrap Up Workshop: Adding an App to Your Business Plan,” Law Seminars International Developing Applications for Mobile Devices Conference, San Francisco, February 14, 2012.](#)

[“Telecom Outlook 2012: Capitalizing on the Market Trajectory,” TelecomHUB, Vienna, VA, January 26, 2012.](#)

[“Our First Take on the FCC’s Universal Service Fund/Intercarrier Compensation Reform Order, Kelley Drye Conference Call, October 28, 2011.](#)

“Employees, Smart Phones and Social Media: Best Practices for Mobile Computing and Social Media Policies,” IAPP Privacy Academy, Dallas, TX, September 15, 2011.

“PII and the Ongoing Data/Privacy Debate,” LeadsCon East 2011, New York, NY, August 25, 2011.

“Mobile Applications: Privacy and Data Security Considerations,” Kelley Drye Webinar, May 16, 2011.

“Privacy & Information Security Update,” American Bar Association Teleseminar, May 4, 2011.

“The State of Carrier/Customer Wholesale Relationships: What’s Working and What Isn’t?,” COMPTEL Spring 2011 Convention & Expo, Las Vegas, NV, March 23, 2011.

“Somebody’s Watching You: Emerging Privacy Issues and their Impact on Service Providers,” COMPTEL Spring 2011 Convention & Expo, Las Vegas, NV, March 21, 2011.

“Working 9-5: Privacy and Data Security Issues for Employers,” 6th Annual Privacy & Data Security Symposium, Washington, D.C., March 16, 2011.

“Kelley Drye Annual USF Update Webinar,” March 2, 2011.

“Privacy By Design, Choice and Transparency: What a New Framework Will Mean for Business and Technology, Washington, D.C., January 20, 2010.

“ECPA’s Wild Ride: 1986 to 2010,” ECPA Reform – Protecting Privacy and Security in the Digital Age, Washington, D.C., September 28, 2010.

“Intercarrier Compensation - A State-Side View,” FCBA CLE, Washington, D.C., May 11, 2010.

“Participating in the FCC’s Vision for the Future Via the National Broadband,” TelecomHUB Event, Vienna, VA, April 21, 2010.

“Federal Universal Service Updated,” Kelley Drye & Warren LLP Webinar, Washington, D.C., March 9, 2010.

“Making Sense of the FCC’s Network Neutrality NPRM,” Presented by Kelley Drye, Washington, D.C., December 2, 2009.

“Privacy Law Paradigm Shift: Policymakers Respond to Rapidly Evolving Technologies,” Kelley Drye & Warren LLP Seminar, Washington, D.C., November 17, 2009.

“Open Internet: Discrimination, Security and Privacy,” CompTel Dallas Show, March 2009.

“Telecom Outlook 2009: Local to Global Perspectives,” TelecomHUB – Tysons Corner, February 2009.

“Federal Regulatory Update: the Year in Review and the Year Ahead,” CompSouth Annual Meeting – Austin, November 2008.

“Navigating Uncharted Waters: Telecom Policy in the Obama Administration and the 111th Congress,” Kelley Drye & Warren LLP Webinar, November 2008.

“Growing Momentum for Electronic Communication Privacy Regulation and Legislation: What to Expect from the Next Congress, Federal Agencies, States and Courts,” Kelley Drye & Warren LLP Seminar, October 2008.

“Key Legal Issues in Telecom Deals – It’s More than Just Price,” CompTel Regional Workshop - Boston, April 2008.

“Wireline Regulatory Issues: Battles Over Switched and Special Access,” CompTel/Kelley Drye & Warren LLP Regulatory Workshop, February 2008.

“Telecom Deals: Legal and Regulatory Considerations for Creating an Exit Strategy,” CompTel Nashville Show, February 2008.

Bar Admissions

District of Columbia, 1997

New York, 1995

Court Admissions

U.S. Court of Appeals – Fourth, Eleventh and District of Columbia Circuits

U.S. District Court – Northern District of Florida

District of Columbia Court of Appeals

State of New York Court of Appeals, 3rd Department

Education

New York University School of Law

J.D., *cum laude*, 1994

NYU Journal of International Law and Politics, articles editor

University of Notre Dame

B.A., *cum laude*, 1989

Notre Dame London Program, Spring 1998

Notre Dame Scholar



Alysa Zeltzer Hutnik

PARTNER

WASHINGTON, D.C.

EMAIL: ahutnik@kelleydrye.com

PHONE: (202) 342-8603

Alysa Hutnik is a partner in the firm's Washington, D.C. office. Her practice includes representing clients in all forms of consumer protection matters, from counseling to defending regulatory investigations and litigation. Her specific focus is on advertising, privacy and data security law.

Ms. Hutnik is past chair of the ABA's Privacy and Information Security Committee (Section of Antitrust Law), the co-chair of the Section's 2011 Consumer Protection Conference, and was the editor-in-chief of the ABA's *Data Security Handbook*, a practical guide for data security legal practitioners.

Prior to joining Kelley Drye, Ms. Hutnik was a federal clerk for the Honorable Joseph R. Goodwin, United States District Judge, Southern District of West Virginia.

Representative Experience

Representing clients in advertising substantiation proceedings, investigations and inquiries from the Federal Trade Commission (FTC); State Attorneys General; the National Advertising Division (NAD); the National Advertising Review Board (NARB); television networks; and federal and state courts and agencies.

Counseling clients regarding compliance with federal and state laws on privacy and data security, including the FTC Act, Gramm-Leach-Bliley Act, the GLB Safeguards Rule, COPPA, FCRA, FACTA, HIPAA, and state privacy and information security laws. Her counseling includes advising companies on the necessary and recommended steps to take following the occurrence of an information security breach, how to design and implement a compliant privacy and information security program, and strategies for contracting with, and providing sufficient and practical oversight and monitoring of, vendors that will be handling personal information on the company's behalf.

Training clients' employees on privacy, data security, advertising and business practices that comply with federal and state consumer protection law, and drafting related marketing guidelines, privacy and data security policies, and employee training materials.

Performing privacy and data security audits of companies' information practices, and assisting companies on identifying and implementing remediation efforts.

Assisting clients in developing and clearing advertising claims and evaluating competitors' conduct for potential advertising challenges.

Representing clients in competitor challenges and consumer protection litigation in state and federal courts, primarily involving on- and off-line retailers, franchisors, technology companies, telecommunications providers and companies that support the financial services industry.

Honors and Awards

Ranked nationally as a leading practitioner in the Privacy & Data Security area by *Chambers USA*, 2008-2011.

Recommended in *US Legal 500* for her work in the Marketing and Advertising and Data Protection and Privacy areas, 2011.

Memberships and Associations

American Bar Association

International Association of Privacy Professionals

Professional Activities

Ms. Hutnik is past chair of the American Bar Association's (ABA) Privacy and Information Security Committee (within the Section of Antitrust), was the editor-in-chief of the ABA's *Data Security Handbook*, a co-chair of the ABA's 2011 Consumer Protection Conference, and has been an editor and contributor to the ABA's newsletter, *The Secure Times*, which addresses privacy and data security legal developments. She is an active member of the ABA's Consumer Protection Committee and regularly organizes teleconferences, brown bags and other meetings for the ABA concerning developments in the law related to advertising, privacy and data security.

Publications

"5 Privacy Tips for Location-Based Services," *Mashable*, January 30, 2012, co-author.

"3 FTC Cases That Could Affect Your Mobile App," *Mashable*, October 21, 2011.

"Why Your App Must Comply With Child Privacy Regulations," *Mashable*, August 18, 2011, co-author.

"Data Security Contract Clauses for Service Provider Arrangements," *Practical Law Company*, July 2011, co-author.

"Senate Hearing Reflects Increasing Focus on Mobile Privacy and Consumer Protection," *E-Commerce Law Report*, June 2011, co-author.

"4 Legal Considerations for Building a Mobile App," *Mashable*, May 26, 2011, co-author.

"Payment Card Data Pass' Rules Gain Some Teeth: An Update on the Legal Landscape," *BNA Privacy & Security Law Report*, March 14, 2011, co-author.

“Congress Explores Consumer Privacy Protection: New Privacy Legislation and FTC Testimony Indicates Direction of Privacy Legislation,” *E-Commerce Law Report*, September 2010, co-author.

“Scrutiny on Payment Card Data Pass: Raising the Profile of Personal Information Sharing Among Marketers,” *BNA Privacy & Security Law Report*, June 2010, co-author.

“Re-Assessing Data Security in 2010: A List of Practical Action Items,” *Metropolitan Corporate Counsel*, May 2010, co-author.

“Representative Boucher Introduces Privacy Legislation,” *e-Commerce Law Report*, Vol. 12, No. 5, May 2010, co-author.

“Red Flags Rule Identity Theft Prevention Program Master Policy,” *Practical Law The Journal*, Vol. 2, Issue 3, April 2010, co-author.

“State Agency Notice Requirements for Data Breaches Chart,” Practical Law Company, April 2010, co-author.

“FTC Warns Companies of Data Leaks on Peer-to-Peer File Sharing Networks,” *Cyberspace Lawyer*, Vol. 15, Issue 2, March 2010, co-author.

“Health IT Law Addresses Interoperability, Privacy, Security And Deployment Of Electronic Health Records,” *Metropolitan Corporate Counsel*, March 2009, co-author.

“Early 2009 Shows Active FTC Data Security Enforcement; No Room For Lax Safeguards,” *Metropolitan Corporate Counsel*, March 2009.

“Data Security Breach Notice Letter,” *PLC Law Department*, February 2010, co-author.

“Common Gaps in Information Security Compliance Checklist,” *PLC Law Department*, February 2010, co-author.

“State Agency Notice Requirements for Data Breaches Chart,” *PLC Law Department*, February 2010, co-author.

“New Massachusetts Data Security Requirements Go Into Effect in January 2009,” *Cyberspace Lawyer*, November 2008, co-author.

“New Connecticut Privacy Law Talks Big but Explains Little,” *Connecticut Lawyer*, October 2008, co-author.
Chair, *Data Security Handbook*, American Bar Association, March 2008.

“State Privacy and Data Protection Laws: Let’s Recap,” *Privacy Tracker*, Vol. 1, No. 1, March 2008.

“Federal Trade Commission holds Town Hall meeting on Behavioral Targeting,” *Privacy and Data Security Law Journal*, Vol. 3, No.1, December 2007, co-author.

“Federal Trade Commission and Banking Authorities Issues Identity Theft and ‘Address Discrepancy’ Rules,” *Privacy and Data Security Law Journal*, Vol. 3, No. 1, December 2007, co-author.

“Privacy and Data Security Update: How to Make Certain the Compliance Checklist Is Up-To-Date,” *Privacy and Data Security Law Journal*, Vol. 2, No. 11, October 2007, co-author.

“Protect Yourself,” *PROMO Magazine*, May 2007, co-author.

“Blogging Do’s and Don’ts,” *Internet Law & Strategy*, February 2007, co-author.

“Corporate Blogging: What to Keep in Mind Before You Start Your Own,” *Computer & Internet*, Andrews Litigation Reporter, Vol. 24, No. 14 (December 2006), co-author.

“New State Privacy Laws: Regulating the Use of Social Security Numbers and Requiring Wireless Security Warnings,” *Privacy and Data Security Law Journal*, Vol. 1, No. 8, December 2006, co-author.

“FTC Settles Privacy Case with Nations Title Agency,” *Privacy and Data Security Law Journal*, July 2006, co-author.

“House Judiciary Committee Passes Data Security Bill,” *Privacy and Data Security Law Journal*, July 2006, co-author.

“Case Closed: Learning from Ten Years of Federal Trade Commission Letters Closing Consumer Protection Cases,” *ABA Consumer Protection Update*, Summer 2006, co-author.

“Identity Theft: What’s a Business to Do When a Consumer Calls to Complain about a Fraudulent Payment?,” *Privacy and Data Law Security Journal*, Vol. 1 No. 6 (May 2006), co-author.

“Product Placement and Brand Integration Strategies: Managing the Risks of Regulatory Uncertainty,” *ABA Consumer Protection Update*, Spring 2006, co-author.

“New Privacy Laws Restricting Use of Social Security Numbers: Is Your Business Compliant?,” *E-Commerce Law and Strategy Journal*, February 2006, co-authored with Scott A. Sinder.

“State Data Breach Laws Are Much Alike, But Differ on Some Key Details,” *BNAs Electronic Commerce and Law Report*, 4 Jan. 2006, co-author.

“Challenging a Competitor’s Advertising Claims,” *The Antitrust Source*, May 2005, co-author.

Speaking Engagements

“Privacy in 2012: What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends,” Kelley Drye Seminar, Washington, D.C., February 16, 2012.

“New Restrictions on U.S. Internet Sales: Data Passes, Negative Opinions, Automatic Renewals and Recurring Charges, American Bar Association Webinar, November 29, 2011.

“How Current Laws and Regulations Apply to Mobile LBS,” FCBA CLE Seminar, Washington, D.C., November 16, 2011.

“Mobile and Handheld Device Gaming,” LSI Gamer Technology Law Conference, Seattle, WA, October 3, 2011.

“Privacy & Data Security Update,” Electronic Funds Transfer Association Legislative & Regulatory Council Meeting, Washington, D.C., September 21, 2011.

“New Restrictions on U.S. Internet Sales: Data Passes, Negative Opinions, Automatic Renewals and Recurring Charges,” American Bar Association Annual Meeting, Toronto, Canada, August 6, 2011.

“Mobile Applications: Privacy and Data Security Considerations,” Kelley Drye Webinar, May 16, 2011.

“Privacy & Information Security Update,” American Bar Association Teleseminar, May 4, 2011.

ABA Consumer Protection Conference, Conference Co-Chair, Washington, D.C., February 3, 2011.

“Privacy By Design, Choice and Transparency: What a New Framework Will Mean for Business and Technology,” Washington, D.C., January 20, 2010.

“Retail Data Privacy: Top Issues Driving Investigations and Litigation, and How to Avoid Becoming a Target,” General Counsel Roundtable, New York, NY, August 4, 2010.

“Privacy and Data Security: Strategies for Avoiding Compliance Gaps, Investigations, and Litigation,” Kelley Drye Continuing Legal Education Seminar, New York, NY, May 5, 2010.

“Privacy Law Paradigm Shift: Policymakers Respond to Rapidly Evolving Technologies,” Presented by Kelley Drye, Washington, D.C., November 17, 2009.

“Privacy and the Law: Legal Insights on Data Privacy Trends and Breach Response,” Bank Info Security Podcast, September 11, 2009.

“Internet and Mobile Commerce Security-Legal and Technical Risks, and Recommended Solutions,” Mobile Commerce Conference – The Midwest Chapter of the Federal Communications Bar Association, Chicago, September 24, 2008.

“Practical Knowledge for the New Technology Landscape,” Electronic Retailing Association Annual Conference, Las Vegas, September 21, 2008.

“Data Security and Privacy: Keeping Your Compliance Checklist On-Track,” Presented by Kelley Drye, Chicago, IL, July 16, 2008.

“Determining the FTC’s Seminal Ability to Pair Traditional Regulations with Emerging Internet, Mobile and Wireless Communications Technologies,” ACI’s 2nd Annual Regulatory Summit for Advertisers and Marketers, Washington, D.C., June 17, 2008.

“What You Need to Know About Privacy and Information Security,” 2008 National Compliance Summit, Presented by October Research Corporation, Las Vegas, NV, February 20, 2008.

“Expert Roundtable Discussion on Blogging Legal Compliance,” 29th Annual Promotion Marketing Association’s Promotion Marketing Law Conference 2007, Chicago, IL, November 16, 2007.

“Data Security and Privacy: Keeping Your Compliance Checklist On-Track,” Presented by Kelley Drye, Vienna, VA, October 30, 2007.

“Federal Enforcement Issues - Shared jurisdiction of the FCC and the FTC,” COMPTTEL Plus 2007 Convention & EXPO, Dallas, TX, October 10, 2007.

“Avoiding Government Scrutiny When Marketing to Wireless Devices,” ACI’s 2nd National Advertisers’ & Marketers’ Regulatory Summit, San Francisco, CA, September 19, 2007.

“Protecting Your Business,” Small Business Webcast Presented by Wells Fargo, May 1, 2007.

“Privacy & Information Security Litigation: An Analysis of Government Enforcement and Private Litigation in 2005-07, and Trends for the Road Ahead,” American Bar Association Section on Antitrust Law, Privacy and Information Security Committee General Session Program, Washington, D.C., April 18, 2007.

“Social Media Update: Legal Implications,” Public Relations Society of America Teleseminar, March 13, 2007.

“What You Need to Know About Privacy and Information Security,” 2007 National Compliance Summit Presented by October Research Corporation, March 1-2, 2007.

“Privacy and Data Security Update,” Kelley Drye Continuing Legal Education Program, February 8, 2007.

“December 2006 Privacy Update,” Monthly Teleseminar Presented by ABA Privacy and Information Security and Corporate Counseling Committees, December 14, 2006.

“Goldilocks and the Three Privacy Bears: Is There Too Much, Too Little or Just the Right Amount of Privacy Law?,” Moderator, ABA Section of Antitrust Law Teleconference, October 25, 2006.

“Privacy and Data Security in Technology Transfers, Complex IP Licensing,” Law Seminars International Conference, McLean, VA, October 17-18, 2006.

“Catching the Fox in the Electronic Henhouse: Preventing, Confronting and Controlling Security Breaches and Identity Theft,” American Bar Association Section on Antitrust Law, Consumer Protection Committee General Session Program, Washington, D.C., March 30, 2006.

“Security Breaches and Data Protection Round Table Discussion,” 27th Annual Promotion Marketing Association’s (PMA) Promotion Marketing Law Conference 2005, Chicago, IL, December 1, 2005.

Bar Admissions

District of Columbia, 2002

Maryland, 2001

Court Admissions

U.S. Court of Appeals – First, Fourth and Ninth Circuits

Education

University of Maryland School of Law

J.D., *Order of the Coif*, 2001

Maryland Law Review, executive editor

Haverford College

B.A., 1998



Gonzalo E. Mon

PARTNER

WASHINGTON, D.C.

EMAIL: gmon@kellydrye.com

PHONE: (202) 342-8576

Gonzalo Mon is a partner in the firm's Washington, D.C. office. Named 2012 D.C. Advertising "Lawyer of the Year" by *Best Lawyers*, his practice focuses on advertising and promotions law.

As an advertising attorney, Mr. Mon works closely with clients who are creative, and he understands that these clients need creative solutions to their problems. As such, he assists clients in designing advertising campaigns, promotions and offers that advance his clients' business goals in a manner that complies with laws and provides as much protection as possible.

Mr. Mon reviews advertisements in television, print, Internet and other media to determine compliance with relevant regulations as well as risk of challenge from competitors and regulators. He has both challenged advertisements on behalf of his clients as well as represented his clients when their own advertisements have been challenged by competitors and regulators.

As companies have begun to use new technologies to promote their brands, Mr. Mon has helped his clients identify and deal with issues raised by these technologies. For example, Mr. Mon regularly helps clients create social media strategies and execute promotions on social media platforms. He also helps clients design and implement various types of mobile promotions.

Mr. Mon has extensive experience in a variety of promotions including sweepstakes, contests, gift cards and loyalty programs. For example, he has worked on instant-win games, text-to-win promotions and contests with user-generated content. In addition to domestic promotions, he has assisted clients with clearing promotions in more than 25 countries worldwide.

Mr. Mon regularly drafts and negotiates various types of promotional agreements. For example, Mr. Mon recently assisted the sponsor of high-profile sweepstakes negotiate agreements with a promotions agency and various prize providers. He has also assisted clients in drafting sponsorship agreements for various sports teams and leagues, including baseball, football, hockey, soccer and even professional bull riding.

Mr. Mon writes extensively on advertising and promotion law issues. His articles have appeared in national publications, such as *PROMO*, *Entertainment Law & Finance*, *Internet Law & Strategy*, *Mobile Marketer*, *Direct Marketing News*, *Journal of Payment Systems Law*, *Internet Retailer*, *ABA Consumer Protection Update*, and *Intellectual Property Today*. Mr. Mon is also frequently invited to speak at events hosted by groups such as the Promotion Marketing Association, the Sales & Marketing Executives International, and various bar associations.

Representative Experience

Assisted a leading travel company in running the largest Facebook promotion in history, including 13 trips and over \$1 million in prizes. Drafted rules for the promotion, coordinated with counsel in the UK and Canada, and drafted agreements with prize providers.

Assisted a quick-service restaurant in structuring and advertising an instant win game offered in conjunction with the release of a major motion picture. Assisted in drafting the official rules, reviewed all advertisements, and negotiated agreements with various prize providers.

Successfully defended a leading company against a lawsuit in which a plaintiff had alleged that one of the company's promotions violated lottery and gambling laws.

Assisted a technology company in developing a contest in which participants were invited to film a commercial for the chance to win a prize. Drafted rules for the promotion, helped protect the company from problematic user-generated content and secured rights to the winning submissions.

Assisted a wireless provider in the design of a sweepstakes in which consumers could enter by sending text messages via their mobile phones. Helped structure the promotions in such a way as to avoid the lawsuits that have recently plagued other companies that have offered text-to-win sweepstakes.

Counseled a retailer regarding the structure of a gift card program, including what terms and conditions could be imposed on card holders. Advised the retailer about its obligations under escheat laws.

Spent more than three years working on-site in a leading Internet company's legal department. Reviewed the majority of the company's advertisements, drafted various agreements, advised on product launches, and assisted with various sweepstakes and contests.

Honors and Awards

Named 2012 D.C. Advertising "Lawyer of the Year" by *The Best Lawyers in America*.

Recommended in *US Legal 500* for his work in the Marketing and Advertising area, 2010 and 2011 and in the Data Protection and Privacy area, 2011.

Memberships and Associations

Promotion Marketing Association

Professional Activities

Judge, Promotion Marketing Association REGGIE Awards, 2012

Publications

“4 Things to Know When Planning a Social Media Contest,” *Mashable*, November 29, 2011.

“5 Legal Considerations for Your Social Media Campaign,” *Mashable*, July 12, 2011.

“Greater Focus on Privacy is Inevitable,” *Mobile Commerce Outlook 2011*, February 2011.

“Can We Say That? A Practical Guide to Substantiating Claims for Food and Consumer Health Products,” *Food and Drug Law Institute Monograph*, Vol 2., No. 3, January 2011, co-author.

“Understanding Legal Challenges on the Mobile Web,” *Mobile Commerce Daily*, October 14, 2010.

“FTC Investigation into a Blogging Promotion Holds Lessons for Advertisers,” *e-Commerce Law Report*, June 2010.

“Apple OKs Promos on iPhones, But Developers Must Comply with Laws,” *Mobile Marketer*, April 20, 2010.

“Expect Additional Legal Challenges as Mobile Matures,” *Mobile Marketer’s Mobile Outlook*, February 2010.

“Facebook Issues New Guidelines For Running Promotions On Its Platform,” *Metropolitan Corporate Counsel*, January 2010.

“New FTC Guides Raise Stakes for Companies that Advertise Through Social Media,” *Marketing Times*, December 2009.

“The Ninth Circuit Holds That Text Messages Are Subject to a Telemarketing Law,” *Intellectual Property & Technology Law Journal*, December 2009.

“Mobile Advertisers Continue to Face Legal Challenges,” *Mobile Marketer’s Classic Guide to Mobile Advertising*, August 2009.

“Rebaters Face More Laws, Enforcement,” *DMNews*, August 2009.

“Focus on Retailers and Rebates,” *ANA Advertiser Online Magazine*, April 2009.

“Contests with Consumer Generated Content Pose Risks As Well As Rewards,” *Marketing Times*, March 2009.

“The Legal Outlook for Mobile: Preparation Helps” *Mobile Marketer’s Mobile Outlook*, March 2009.

“Contests With Consumer-Generated Content Pose Risks as Well as Rewards” *Marketing Watchdog Journal*, March 2009.

“New Settlements Suggest Online Retailers Should Focus on Web Site Accessibility,” *E-Commerce Law & Strategy*, December 2008.

“Mobile Sellers Face Technological and Legal Challenges,” *Classic Guide to Mobile Commerce*, November 2008.

- “Legal Checkup,” *PROMO Magazine*, September 2008.
- “Wireless Wilderness,” *PROMO Magazine*, July 2008.
- “The Risky Business of Consumer-Generated Content,” *Incentive*, May 2008.
- “If You’re Not Careful, Consumer Generated Content Can Lead to Risky Business,” *OMMA*, May 2008.
- “Navigating Gift Card Regulations: As Gift Card Sales Increase, So Do the Legal Hurdles,” *Incentive Magazine*, April 2008.
- “Handling Consumer-generated Content Without Getting Burned,” *e-Commerce Law Report*, March 2008.
- “Consumer-Generated Content Got You BURNED?” *ADOTAS*, March 2008.
- “Consumer-Generated Content is Hot,” *Entertainment Law & Finance*, May 2007, with David Ervin.
- “Protect Yourself,” *PROMO Magazine*, May 2007, with Alysa Zeltzer.
- “New Laws Continue to Complicate Gift Card Programs,” *The Metropolitan Corporate Counsel*, January 2007.
- “Tangled Local Regs Dictate National Promotions,” *Promo Magazine Special Report*, October 2006.
- “State Consumer Protection Laws Constrain Gift Card Issuers,” *Journal of Payment Systems Law*, March/April 2006.
- “Ins and Outs of Sweepstakes Law,” *DM News Online*, March 6, 2006.
- “CAN-SPAM’s Effect on Viral Marketing,” *DM News*, May 1, 2004 (co-authored with John P. Feldman).
- “States Scrutinize Gift Certificates,” *Promo Magazine*, November 2003 (co-authored with John P. Feldman).
- “Headaches the Generic Brand Can’t Relieve,” *Intellectual Property Today*, October 2003 (co-authored with John P. Feldman).
- “When Good Promotions Go Bad,” *Promo Magazine*, June 2003 (co-authored with John P. Feldman).
- “FTC’s Big-Bucks Children’s Privacy Settlements Send a Message to all Online Marketers,” *Internet Retailer*, May 2003 (co-authored with John P. Feldman).
- “Avoid the Pitfalls of Online Coupons,” *DM News*, April 7, 2003 (co-authored with John P. Feldman).
- “When the FTC Comes Calling, Retailers Have to be Aware of More than just Shipping Rules,” *Internet Retailer*, February 2003.
- “Marketing Sweepstakes Via the Mail,” *DM News*, September 23, 2002.
- “Listing Towards Privacy: List Brokers and Owners May Be the Government’s Next Targets,” *Promo Magazine*, May 2002 (co-authored with D. Reed Freeman Jr.).

“E-Mail Marketing Under UCE Statutes,” *DM News*, May 13, 2002.

“No New Year’s Celebration For Email Marketers,” *ABA Consumer Protection Update*, Spring 2002.

“Buying from the Heart: Rules for Charitable Promotions,” *ABA Consumer Protection Update*, Fall 2001.

“What You Need to Know About the Mail Order Rule,” *National Mail Order Association Newsletter*, December 2001.

“New Trend in Interactive Ads Raises Legal Questions,” *Sales and Marketing Strategies and News*, November 2001 (co-authored with John P. Feldman).

“Advertainment and Advergaming: Legal Considerations Concerning a New Trend in Online Advertising,” *E-Commerce Law Report*, September 2001 (co-authored with John P. Feldman).

“Are E-Mail Referral Programs Spam?,” *iMarketing News*, March 27, 2001 (co-authored with Adam Cramer).

“Running a COPPA-Compliant Sweepstakes,” *E-Commerce Law Report*, March 2001 (co-authored with John P. Feldman).

Speaking Engagements

“How Has Social Media Changed the Landscape?,” Consumer Product Marketing, Advertising, Distribution, and Sales Law Conference, Boston, MA, March 23, 2012.

“What’s in a Natural or Organic Claim: Preventing Common Pitfalls that Can Lead to Private Consumer Litigation and Downstream Government Enforcement,” ACI 2nd Advanced Legal Summit on Food & Beverage Marketing & Advertising, Washington, D.C., March 19, 2012.

“Privacy in 2012: What to Watch Regarding COPPA, Mobile Apps, and Evolving Law Enforcement and Public Policy Trends,” Kelley Drye Seminar, Washington, D.C., February 16, 2012.

“Marketing and Advertising through Social Media: Key Legal Issues and Strategies for In-house Counsel,” Practical Law Company Webinar, December 7, 2011.

“Mobile Marketing: The Legal Landscape,” FedCollege Corporate College Recruiting Conference, Washington, D.C., December 7, 2011.

“Social Media for Business: Boon or Bane?,” The Knowledge Congress Webcast, December 6, 2011.

“We Know Where You Are – Developing and Using Location Based Apps,” 33rd Annual PMA Marketing Law Conference, Chicago, IL, November 15, 2011.

“Mobile Marketing: Navigating The Legal Landscape,” mRecruitingCamp, San Francisco, CA, September 30, 2011.

“Marketing and Advertising Through Social Media: Key Legal Issues and Strategies for In-House Counsel,” ACC Luncheon Program, Chicago, IL, September 21, 2011.

“Trending Topics: Social Media and the Law,” Kelley Drye Webinar, August 9, 2011.

“May 2011 Consumer Protection Update,” American Bar Association Teleconference, June 20, 2011.

“Comparative Advertising-Claim Substantiation,” Promotional Marketing Association 32nd Annual Marketing Law Conference, Chicago, IL, November 18, 2010.

“A New Legal Frontier for Social Media,” Kelley Drye Continuing Legal Education Seminar, New York, NY, March 10, 2010.

“A New Legal Frontier for Social Media,” Kelley Drye Continuing Legal Education Seminar, New York, NY, February 9, 2010.

“Mobile Marketing – The Third Screen,” 31st Annual Promotion Marketing Law Conference, Chicago, IL, November 5, 2009.

“Legal Do’s and Don’ts with Mobile Marketing Campaigns,” Mobile Marketing for Agencies and Media Buyers, New York, NY, April 29, 2009.

“Handling Consumer-Generated Content Without Getting Burned,” Social Media Road Show Conference, Boston, MA, February 26, 2009.

“The Basics of Structuring Promotions and Integrated Marketing Campaigns,” 30th Annual Promotion Marketing Association Law Conference, Chicago, IL, November 20, 2008.

“How to Benefit from User-Generated Content While Reducing the Risks,” Kelley Drye Continuing Legal Education Seminar, New York, NY, October 7, 2008.

“Avoiding a Promotion Commotion: Rebates, Gift Cards, and other Promotional Practices,” Conference on Advertising Law: FTC Rules of the Road, Colorado Bar Association, Denver, CO, July 24, 2008.

“Mobile Marketing and Consumer Generated Content,” Technology and Marketing Committee of the Westchester/Fairfield (WESFACCA) Chapter of the American Corporate Counsel Association, Stamford, CT, April 9, 2008.

“Marketing to Wireless Devices,” Promotion Marketing Association’s Who’s In Control Now Conference, Chicago, IL, December 15-16, 2007.

“Basic Legal Principles of Advertising and Billing for In-House Counsel,” Kelley Drye Continuing Legal Education Seminar, New York, NY, May 1, 2007.

“December 2006 Privacy Update,” Monthly Teleseminar Presented by ABA Privacy and Information Security and Corporate Counseling Committees, December 14, 2006.

“Just for Rookies: A Workshop for Beginners,” Promotion Marketing Association’s *Hitting the Target: Platforms & Protocols for Reaching Consumers*, Chicago, IL, December 12-13, 2006.

“The Real World of Promotions,” Promotion Marketing Association’s Reality Check, Chicago, IL, December 2-3, 2004.

“The Changing World of Advertising,” Promotion Marketing Association’s Annual Conference, New York, NY March 2004.

Bar Admissions

District of Columbia, 2001

Virginia, 2000

Education

George Washington University Law School

J.D., 2000

College of New Jersey

B.A., *magna cum laude*, 1996

Language Capability

Spanish

Supplemental Resources

Please reference the enclosed flash drive for the following supplemental resources:

Children's Privacy Resources

- Children's Privacy in the Mobile Data Environment
- Disney COPPA Rule Comment
- FTC COPPA Rule
- FTC Notice on Facial Recognition Technology
- FTC Releases Proposed Revisions to COPPA
- Jessica Rich Statement on Children's Privacy
- Jessica Rich Testimony – Protecting Youths in an Online World
- TRUSTe COPPA Rule Comment
- Why Your App Must Comply with Child Privacy Regulations

Mobile Apps and Location-Based Services Resources

- 4 Legal Considerations for Building a Mobile App
- 5 Privacy Tips for Location-Based Services
- CDT and FPF Mobile App Developer Best Practices
- CTIA LBS Best Practices
- Developing and Using Location-Based Apps
- FCC Public Notice LBS Forum
- FTC Frostwire Order
- FTC Letter to Everify Regarding Mobile Apps
- FTC Letter to InfoPay Regarding Mobile Apps
- FTC Letter to Intelligator Regarding Mobile Apps
- FTC Prepared Statement before Senate on Mobile Privacy
- FTC W3 Order
- Google Response to FCC LBS Forum
- MMA Mobile Advertising Guidelines
- MMA Mobile Application Privacy Policy Framework
- Swire FCC Forum Wrap Up on Privacy and LBS
- TRUSTe Location Aware Mobile Apps Best Practices

DataGuidance is the leading global data protection and privacy compliance resource tool, created with a single aim - to make data protection and privacy compliance simpler. It delivers, in one site, legal and regulatory information from all relevant data protection and privacy sources, keeping its growing community of subscribers on top of national laws and regulations, in a quick, easy to navigate, clear database. In addition, DataGuidance Notes and At-A-Glance Advisories are devised by data protection experts to provide users with advice on both global coverage and local compliance.

DataGuidance subscribers include: Citigroup, BP, Rolls Royce, Proctor & Gamble, IBM, AmGen

This article was originally published in DataGuidance, October 2011.

Children's Privacy in the Mobile Data Environment

Recent evidence suggests that children, including children as young as three and four years of age, increasingly use mobile devices to access the Internet to play games, communicate with peers, or engage in interactive content targeting a young audience. Studies by the Pew Internet and American Life Project, for example, found that 58 percent of 12 year olds in the United States have access to cell phones,¹ and 46 percent use social networking services.² Further, a recent report by Nielsen Research found that games and social networking — the two most attractive online activities for children — represent two of the three most popular mobile app categories.³ These statistics portend a range of issues relating to children's online privacy, including parental notice, consent and verification, third-party access to children's personal information, and the collection and use of geolocational data obtained from a mobile device.

This article describes the recent legal and regulatory developments that directly affect children's privacy protections in the mobile data environment. The article also includes practical considerations for businesses that develop mobile content targeted to children.



Dana B. Rosenfeld
Partner
Kelley Drye & Warren LLP



Matthew P. Sullivan
Associate
Kelley Drye & Warren LLP

¹ Kristin Purcell et al, *Pew Internet and American Life Project – The Rise of Apps Culture*, Pew Research Center (Sept. 15, 2010).

² Amanda Lenhart et al, *Pew Internet and American Life Project – Social Media and Young Adults*, Pew Research Center (Feb. 3, 2010).

³ Nielsen Research, *Play Before Work: Games Most Popular Mobile App Category in US*, NielsenWire (Jul. 6, 2011), available at http://blog.nielsen.com/nielsenwire/online_mobile/games-most-popular-mobile-app-category/.

Why the Mobile Environment is Different

The mobile platform has become a critical gateway to the Internet, due primarily to the rapid growth of the mobile app industry, and the evolving use of social media. In light of these developments, parents, lawmakers, and regulators are placing an increased focus on the privacy risks associated with children's participation in the mobile Internet.

The mobile environment has several elements that raise unique concerns with respect to children's privacy. For example, unlike personal computers, which are tethered to home or school, most people carry their mobile device or smartphone with them at all times. These devices continually generate geolocation data that leave a virtual breadcrumb trail of the users' whereabouts. This location information may then be accessed by mobile device service providers or third-parties, such as mobile app developers. Further, the screen sizes found on most mobile devices do not lend themselves to the same type of lengthy consumer notices concerning privacy and collection of personal information that can be displayed on personal computer screens. Finally, mobile app developers generally are not legally required to include privacy policies within their applications, so consumers may not be aware of the manner or extent to which personal information collection is occurring.

Legislators Consider Children's Online Privacy Protections

Federal lawmakers have taken notice of the unique concerns with respect to mobile data and children's privacy. Among the 18 consumer privacy bills that have been introduced by Congress so far this year, a number of them directly address children's online privacy or the mobile data environment. In May 2011, Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX) introduced the Do Not Track Kids Act of 2011 (H.R. 1895). The bill would prohibit the operator of an online service or mobile application from compiling or disclosing to third parties personal information collected from children under 13 and minors (children between the ages of 13 and 17) for targeted marketing purposes. The bill also would restrict the collection of geolocation information for children and minors.

In June 2011, members of the House and Senate introduced several bills intended to restrict the use of consumer geolocation information. The bills include the Geolocation Privacy and Surveillance Act ("GPS Act") (H.R. 2168) introduced by Rep. Jason Chaffetz (R-UT) and Rep. Robert Goodlatte (R-VA), and the Location Privacy Protection Act of 2011 (S. 1223) introduced by Sen. Al Franken (D-MN) and Sen. Richard Blumenthal (D-CT). Both bills prohibit the collection, use, or disclosure of consumer geolocation data without consumer consent, and would extend protections to both real-time and archived geolocation information. The bills include only a small number of exceptions for undisclosed use of such data, including in emergency situations. Notably, both bills would impose criminal and civil penalties for unlawful collection, use or disclosure of a consumer's location data.

Lawmakers' sense of urgency has been driven, in part, by news reports concerning the unauthorized collection of consumers' location information stored on mobile devices as well as several recent high-profile data breaches. In April 2011, for example, Sony announced that hackers had compromised the personal information of more than 75 million PlayStation users. The same month, news reports surfaced that Apple's iPhone and Google's Android devices were storing device location information without users' knowledge or consent. Legislators responded with a series of hearings in late Spring that included testimony from both industry representatives, including Apple and Google, and federal regulators. On May 10, 2011, the U.S. Senate Judiciary Subcommittee on Privacy, Technology and the Law held the hearing "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phone and Your Privacy." During the hearing, Jessica Rich, Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC") testified that FTC Staff was engaged in "a number of active investigations into privacy issues associated with mobile devices, including children's privacy."

FTC to Update the Children’s Online Privacy Protection Rule

The primary mechanism for safeguarding children’s online information is the Children’s Online Privacy Protection Rule (“COPPA Rule” or “Rule”).⁴ The Rule, which was enacted in 1998, requires commercial websites and online services that target children to provide direct notice to a parent and obtain the parent’s verifiable consent before collecting personal information from children under the age of 13.

In September 2011, the FTC issued proposed amendments to the Rule that are intended to address the substantial changes in consumer technology that have occurred over the past decade since the Rule first went into effect. The proposed revisions are designed to ensure that the Rule continues to provide privacy protections for children who increasingly participate in social networking and interactive gaming, or engage in online activities through a mobile device.

COPPA Rule Definitions

Among the notable proposed changes to the Rule, the FTC is seeking to expand the Rule’s definition of “personal information” to include new forms of data that the FTC considers personally identifiable. Under the proposed revisions, “personal information” would include online screen and user names, unless the names are used for technical maintenance of the online service or website. In recognition of information-sharing trends on social media sites, the revised definition also would cover photographs, and video or audio files containing a child’s image or voice. Notably, the FTC is proposing that “personal information” also include geolocation information emitted by a child’s mobile or electronic device. This proposed revision responds to the recent concerns expressed by Congress and the FTC over the extent to which mobile operators are collecting location information from user devices.

Parental Notice and Consent

The proposed rule would address space constraints associated with most mobile device screens by limiting the use of lengthy privacy policies to communicate information to parents and kids, and streamlining the current notice requirements. This proposed approach would require that mobile application developers, for example, give parents easy-to-understand information provided on a real-time basis, which is consistent with the FTC’s preference that disclosure and notice information be “embedded in the interaction.”

The FTC’s recognition of new technologies is evident in the proposed changes to the consent requirements in the current rule. For example, the Commission’s proposal would expand the methods by which operators can seek and obtain verifiable parental consent to include electronically-scanned versions of signed parental consent forms, videoconferencing, and government-issued identification – such as a driver’s license – that is checked against a database. The Commission also hopes to stimulate the development of new technology-based methods of consent and is proposing a new process through which operators may voluntarily seek FTC approval of potential consent mechanisms. Prior to approval, the FTC would review the mechanism and offer it for public comment.

Security Safeguards

The COPPA Rule requires operators to establish reasonable procedures to protect the confidentiality and security of children’s personal information; however, the current rule is silent on the data security obligations of third parties. The proposed revisions would require that companies take “reasonable measures” to ensure that any service provider or third party to whom children’s personal information is provided has enacted “reasonable procedures” to protect the confidentiality and security of such information.

⁴ 16 C.F.R. Part 312

The proposed revisions also would impose a new data retention and deletion requirement, whereby companies could retain children's personal information only for so long as it reasonably necessary to fulfill the purpose for which the information was collected. The operator also would be required to take reasonable measures to protect against unauthorized access to the information during the data deletion or disposal process.

COPPA Rule Enforcement

In addition to its rulemaking authority, the FTC is also using its enforcement powers to safeguard children's online privacy. The FTC, within the past several months, has announced a number of settlements with mobile app developers, including those that offer content targeted to children. In August 2011, for example, the FTC announced that it had reached a settlement in its first action against a mobile applications ("app") developer. The FTC had charged W3 Innovations, LLC ("W3") and its President with violating the COPPA Rule when W3 allegedly collected and disclosed personal information from up to 30,000 children without their parents' consent.

W3 Innovations, which does business as Broken Thumbs Apps, develops and distributes apps including Emily's Girl World and Emily's Runway High Fashion (the "Emily Apps"), which are sold through the "Games-Kids" section of Apple, Inc.'s App Store. According to the FTC Complaint, the Emily Apps encouraged children to submit emails, including messages to friends and requests for advice, that were then posted as publicly-available blog entries to the "Emily's blog" feature on the Emily Apps sites. Children also could submit comments to the site using a form that required user name and email address information. The settlement requires W3 and its president to pay \$50,000, and they must delete all personal information collected in violation of COPPA.

Practical Considerations for Businesses

Given the current focus on children's privacy by regulators and legislators, companies seeking to enter the mobile app market or engage a younger audience using games or other online features should keep in mind several best practices that can help reduce risks resulting from increased legal and regulatory scrutiny.

- **Know your/your partner's app** – Before launching your mobile app, ensure that all stakeholders fully understand the extent to which the app collects, uses, and disposes of personal information. Evaluate whether any benefits associated with any information collections are worth the increased scrutiny. If you are partnering with other companies, ensure that you have a full understanding of their app and business model and appropriately allocate risk through express contractual requirements and liabilities.
- **Understand the COPPA Rule** - Don't be caught off-guard by learning *after* a regulatory inquiry that your business activities fall within the parameters of the COPPA Rule. For example, the Rule, in addition to covering websites that target kids directly, also applies to an online service that targets a general audience if that company has actual knowledge that it is collecting or maintaining personal information from a child.
- **Closely track the proposed COPPA Rule revisions as well as legislative developments** –Many of the FTC's proposed revisions likely will be part of the final revised Rule. Some of the proposed revisions could add substantial new obligations to certain parties. For example, multiple parties, including app developers, ad networks, and service providers are responsible for different functions in delivering the app to the consumer. A proposed revision would modify online notice requirements by mandating that *all* operators involved in the operation of an online service – and not just a designated operator, as permitted under the current Rule – provide contact information that includes the operator's name, physical address, telephone number an email address.

Conclusion

The mobile environment has opened up a dynamic sales channel for app developers that create content targeting a young audience. Businesses that seek to participate in this market, however, must remain mindful of the scrutiny given to children's privacy and the unique characteristics of the mobile data environment, understand and follow the COPPA Rule, and closely monitor ongoing regulatory and legislative developments specifically targeting this growing market segment.

* * *

Dana B. Rosenfeld is chair of the Privacy & Information Security practice and partner in the Advertising & Marketing practice at Kelley Drye & Warren LLP in Washington, D.C. Matthew P. Sullivan is an associate in the Advertising & Marketing and Privacy & Information practices at Kelley Drye.

December 23, 2011

VIA ONLINE SUBMISSION

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

RE: In the Matter of COPPA Rule Review, 16 CFR Part 312, Project No. P-104503

The Walt Disney Company (“Disney”) is pleased to submit these comments in response to the Federal Trade Commission’s (“FTC”) request for comments on proposed revisions to the Children’s Online Privacy Protection Act (“COPPA”) Rule.¹ Disney’s comments, which are intended to provide constructive feedback on the COPPA Rule and the Commission’s proposed changes to it, are framed in part by changes in the Internet experience, an analysis of how the online industry, parents, and children have responded to the existing COPPA framework over the past several years, and the practical effect that this has had on fulfilling COPPA’s privacy objectives under the current Rule. Disney also provides these comments in light of its role as a provider of family entertainment and premium content on and off the Internet, and its commitment to achieving the privacy goals of COPPA and the FTC.

Disney’s comments address how the COPPA Rule and the FTC’s proposed revisions to it would affect, in particular, family-friendly websites and online services that attract users of all ages, and concerns over the extent to which the proposed Rule changes may inadvertently affect online innovation and children’s privacy protections going forward. The comments introduce several solutions for the Commission’s consideration that would meet the Commission’s objective for furthering the Rule’s privacy goals. Specifically, Disney proposes an expanded approach that aims to: better protect children’s privacy and encourage parental engagement in light of the reality of children’s current Internet use; provide online operators that offer content and services that appeal to families with appropriate incentives to invest in both child-oriented content and an engaging family context; and result in a greater number of online services that proactively protect the privacy of children where they now traverse the Internet. The comments further set forth legal frameworks within COPPA by which the Commission can implement Disney’s proposed solutions.

In addition, the comments also describe new parental verification mechanisms that can leverage current platform technologies to improve transparency and parental control, and we encourage the Commission to use its leadership position to foster continued dialogue between industry and consumers on new verification solutions. Lastly, the comments highlight proposed

¹ Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312.

changes to definitions within the Rule that Disney believes would benefit from further modification, clarification, or review.

I. The State of Children's Online Privacy

A. COPPA's Early Legacy

The ongoing and rapid evolution of the Internet during the past ten years — recently punctuated by the broad adoption of social networking and mobile platforms and an increase in the amount of time that people of all ages spend online — has proven the FTC prescient when it supported Congressional efforts in the late 1990s to pass children's online privacy protection legislation. In 1997, only 3.5 million U.S. children ages 12 and under were online,² which represents a fraction of the more than 20 million children under age 11 who are online today,³ or the 25.7 million children expected to be online by 2015.⁴ Moreover, when COPPA was enacted in 1998, digital media, interactive games and activities, social media, and the mobile Internet were still nascent forms of communication, and online interaction was limited primarily to chat rooms, instant messaging, and email accessed through a family's home desktop computer. Nevertheless, the FTC rightly recognized that emerging web-based information collection practices had “real world consequences for family privacy and security.”⁵

The Commission's support for COPPA was largely a response to two principal concerns: (1) children's personal safety and protection from online predators in light of the increased access to children's personal information; and (2) parents' lack of visibility with respect to the information that online merchants were collecting from children using active methods (questions posed directly to children online) and passive methods (persistent identifiers such as cookies). The Commission's concerns were based on its own survey research involving more than 1,400 websites, which showed that few websites directed to children had meaningful mechanisms to engage parents before collecting their children's information.⁶ In addition to these concerns, the FTC was mindful about ensuring that the COPPA Rule maintained children's access to the Internet, preserved the interactivity of the online medium, and minimized the burdens of compliance on companies, parents, and children.⁷ In response to these concerns and objectives, and pursuant to the COPPA statute, the FTC implemented the COPPA Rule in April 2000.

² *Protection of Children's Privacy on the World Wide Web Before the Subcomm. On Commerce, Science, and Transportation of the Sen. Comm. On Commerce, Science and Transportation* (Sept. 23, 1998) (statement of Robert Pitofsky, Chairman, Federal Trade Commission).

³ Stephanie Reese, *Report Roundup – Demographics*, eMarketer (Mar. 21, 2011), available at <http://www.emarketer.com/blog/index.php/tag/number-of-children-online/>.

⁴ *Id.*

⁵ Pitofsky (Sept. 23, 1998).

⁶ Martha K. Landesberg, Toby Milgrom Levin, Caroline G. Curtin, Ori Lev, *Privacy Online: A Report to Congress*, Federal Trade Commission (June 1998) at iii.

⁷ Children's Online Privacy Protection Rule; Final Rule, 64 Fed. Reg. 59889 (Nov. 3, 1999).

In 2006, the FTC declined to modify the COPPA Rule after concluding that the Rule provided “a workable system” to help protect the online safety and privacy of children using the Internet.⁸ Among its findings, the Commission determined that the Rule did not adversely affect the number of websites directed to children and had proven “effective in applying [its] flexible standard . . . to new online services.”⁹ The Commission, however, was cognizant of the initial shifts in Internet use trends brought about by the availability of new services and platforms and the convergence of wireless and landline communications with the Internet.¹⁰ Indeed, the FTC recently cited these factors as the rationale for the current accelerated review of the COPPA Rule.¹¹

B. As the Internet Has Evolved, the COPPA Rule Has Resulted in Unintended Consequences that Do Not Advance the FTC’s COPPA Objectives

As noted above, the FTC originally sought to structure the COPPA Rule to ensure that it would maintain children’s access to the Internet, encourage the interactivity of the online medium, and minimize the burdens of compliance on companies, parents, and children.¹² In 1998, for example, the Commission recognized that “the Internet presents children with an extraordinary new means to tap into rich sources of information that previously were difficult to access, and to communicate with their peers and others in ways never before imaginable.”¹³ Yet even with the technological advancements at that point in time, the FTC could not have anticipated the extent to which the Internet would soon be interwoven in daily life, how consumers of all ages would embrace online services and new platforms, or the degree to which consumers would come to expect and demand increasingly interactive online content.

The extent to which children now use the Internet, including the wide variety of online services and social networks not specifically designed for them and available through a variety of platforms, is a prime example of user trends that could not have been anticipated when the COPPA Rule was first promulgated. Today, 22 percent of children between the ages of 5 and 8 use a computer at least once a day, with another 46 percent who use a computer at least once a week, to watch videos, play video games, or listen to music.¹⁴ Indeed, research published in

⁸ *Consumer Privacy on the World Wide Web Before the Subcomm. On Telecommunications, Trade and Consumer Protection of the H. Comm. On Commerce* (July 21, 1998) (statement by Robert Pitofsky, Chairman, Federal Trade Commission) at p.28.

⁹ *Implementing the Children’s Online Privacy Protection Act*, Federal Trade Commission Report to Congress (Feb. 2007) at 2.

¹⁰ *Id.* at 27.

¹¹ *An Examination of Children’s Privacy: New Technology and the Children’s Online Privacy Protection Rule Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. On Commerce, Science and Transportation* (statement by Jessica Rich, Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission) (Apr. 2010).

¹² Children’s Online Privacy Protection Rule; Final Rule, 64 Fed. Reg. 59889 (Nov. 3, 1999).

¹³ Pitofsky (Sept. 23, 1998).

¹⁴ Common Sense Media, *Zero to Eight: Children’s Media Use in America* (Fall 2011), available at <http://www.common sense media.org/sites/default/files/research/zerotoeightfinal2011.pdf>.

2011 shows that children between the ages of 8 and 10 spend at least 46 minutes each day on a computer, with the primary activities including social networking, playing games, visiting websites, and watching online videos.¹⁵ Children also are increasingly using mobile devices to access online services. Eleven percent of all children between the ages of 0 and 8 use a cell phone, Mp3 music player, mobile tablet, or similar device for media consumption, spending an average of 43 minutes each day on these devices.¹⁶ Notably, the wireless mobile tablet is the most desired consumer electronic product among children for the holiday season of 2011, with interest in the tablet significantly greater among younger children (44 percent for children ages 6-12), than it is for consumers age 13 and older (24 percent).¹⁷

In short, the Internet is now inextricably woven into the fabric of daily life for most families. Moreover, as the Internet has become increasingly embedded in the household, social norms with respect to Internet use have shifted, and the content viewed online is increasingly done so in a multi-generational context. In 2008, the Pew Research Center conducted a study which found that technology is enabling new forms of family connectedness that revolve around “communal Internet experiences.”¹⁸ Twenty-five percent of respondents in the study said that their family is closer, in part, due to the Internet, versus less than 14 percent who said that the Internet has contributed to the family becoming more distant.¹⁹ A prime example of this multi-generational dynamic is the online video game industry, where the average player is 33 years old. A 2007 survey of adult “gamers” — including parents who themselves grew up playing video games — indicated that 27 percent of the respondents spend more than one hour per week playing online video games together with their children.²⁰

The evolving patterns of Internet use among family members, coupled with the emergence of highly-interactive online platforms, inevitably means that more children frequent general audience online sites that are not designed for or directed to children. Importantly, evidence suggests that these trends are consistent with parent’s expectations. Forty-five percent of 12-year old children now use a social network site to communicate with friends and family,²¹ and many do so with their parents’ direct involvement and consent. Panelists in the FTC’s 2010 COPPA Rule Review Roundtable, for example, described parents’ desire for their children to

¹⁵ Victoria J. Rideout, Ulla G. Foehr, and Donald F. Roberts, *Generation M² – Media in the Lives of 8- to 18-Year Olds*, Kaiser Family Foundation (Jan. 2010).

¹⁶ Common Sense Media (Fall 2011) at 9.

¹⁷ Nielsenwire, *U.S. Kids Looking Forward to “iHoliday” 2011* (Nov. 17, 2011), available at <http://blog.nielsen.com/nielsenwire/consumer/us-kids-looking-forward-to-iholiday-2011/>.

¹⁸ Tracy L.M. Kennedy, Aaron Smith, Amy Tracy Wells, Barry Wellman, *Networked Families: Parents and Spouses Are Using the Internet and Cell Phones to Create a “New Connectedness” that Builds on Remote Connections and Shared Internet Experiences*, Pew Internet & American Life Project (Oct. 19, 2008)

¹⁹ *Id.* at 29.

²⁰ Alexandra Macgill, *Is Video Gaming Becoming the Next Family Bonding Activity?*, Pew Research Center (Nov. 19, 2007).

²¹ Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, Lee Rainie, *Teens, Kindness and Cruelty on Social Network Sites*, Pew Research Center (Nov. 9, 2011) at 17.

more easily connect with family members as a catalyst for young children to create accounts on general audience social network sites.²²

Similarly, in a recent national study of parents with children ages 10-14 that was presented in the peer-reviewed online journal *First Monday*, 78 percent of the respondents believed that communicating with family and friends, educational purposes, and keeping pace with classmates' online habits provided adequate justification for a child to register for an online service even if the child does not meet the minimum age requirements.²³ The survey, which was conducted by researchers at Harvard, Northwestern, New York University, and University of California, Berkeley, also revealed that more than half of the parents with a 12-year old child were aware that their child maintained a social networking site account — 82 percent of the parents knew when their child had registered their account, and 76 percent of the parents assisted the child in creating the account.²⁴ In questioning the efficacy of the current COPPA framework in light of children's gravitation to Internet content not directed to them, the researchers noted that most parents prefer “an emphasis on better mechanisms for getting parents involved in [children's online privacy] while only about a tenth wanted the focus to be on restricting access for children.”²⁵ In other words, most parents want enhanced transparency and parental control with respect to their child's use of general audience websites and online services, rather than restrictions against using them.

In addition to the types of websites and online services now used by children, how online content is accessed and delivered also has changed. Today, online content and services are developed and delivered through a variety of systems, platforms and devices, largely as a result of collaboration among numerous entities, including content providers, Internet-based platforms, telecommunications carriers, device manufacturers, mobile and desktop application developers, and service providers. This multi-party structure, while expanding innovation and enabling new types of online services, features, and accessibility, presents challenges for how a website operator can address transparency and parental control under COPPA. Namely, not all parties in this multi-party structure have incentives under COPPA to invest in transparency and parental control tools, but their efforts and investment are necessary for development of an ecosystem that enables operators to effectively develop and deliver services that best meet the goals of COPPA. Collaboration also is important to ensure that these same principles are achieved regardless of which platform, device or other means in which the online service or site is accessed by the user. Not surprisingly then, it is this collaborative group of entities that may be best-positioned to leverage the cooperative nature of service delivery and implement real-time communications

²² COPPA Rule Review Roundtable, Wed. June 2, 2010 (Comments of Denise Tayloe) at p. 119. (“[T]here are people who advocate kids shouldn't be on social networks, but there are lots of parents who want their kids to have a Facebook account to talk to their cousin or talk to their father who's in the military or whoever it might be . . .”).

²³ Danah Boyd, Eszter Hargittai, Jason Schultz, John Palfrey, *What Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act*, *First Monday* (Nov. 7, 2011) at p. 15.

²⁴ *Id.* at pp. 11-13.

²⁵ *Id.* at p. 22.

with parents, robust parental controls, and innovative platform-based consent mechanisms, provided that adequate incentives exist to encourage investment in these areas.

User expectations regarding speed and ease of use of online services and content also have evolved. Operators are keenly aware that consumers will quickly move on if websites are slow to load, functionality is delayed, or registration-type processes stand between users and their content. Unfortunately, the reality is that parental permission processes themselves can discourage children from accessing services, driving them instead to services that are accessible immediately and without permission processes that result in delay. This reality further discourages operators from seeking to determine which of their users are children.

In addition to these challenges, there is an inherent ambiguity as to whether some websites and online services are in fact “directed to children” because they involve one or more of the factors under the COPPA Rule’s “totality of factors” test.²⁶ And because the COPPA Rule’s implementing requirements that apply to “websites directed to children” do not work well for websites and online services that are used by individuals of all ages (providing a potentially confusing and poor user experience by treating all users as children for the reasons described above), the result is that operators may seek to avoid populating their websites and online services with content that even potentially could be considered family-friendly and, thus, potentially “directed to children.”

Accordingly, the current COPPA framework does not provide incentives for operators to invest in websites and online services that are “directed to children” or those that may be construed as a “website or online service directed to children” based on some interpretations of the “totality of factors” test. This also means that many operators do not invest in solutions for online transparency and parental controls as originally intended by COPPA. Nor do they actively practice data minimization by limiting the need for the collection of personal information at the outset. Rather, the reality is that operators have strong incentives to comply with COPPA by designing their online websites and services so that the sites and services are clearly *not* directed to children, and for the operators to either avoid actual knowledge of a user’s age or block children from participating in their service or accessing their site. Indeed, at present, it is far easier for operators to exclude family-friendly content on their websites and online services, and to avoid actual knowledge of a user’s age or restrict users to those over age 12, than to invest in data minimization and parental consent mechanisms and engender the risk of potential violations under COPPA.

The *First Monday* researchers noted this paradox created by what they termed as “fundamental flaws” in COPPA’s design:

²⁶ Children’s Online Privacy Protection Rule, 16 CFR 312.2 (within the definition of “website or online service directed to children,” the Rule provides that “*In determining whether a commercial website or online service, or a portion thereof, is targeted to children, the Commission will consider the subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities.*”)(current, non-amended version).

By creating this environment, COPPA inadvertently hampers the very population it seeks to assist and forces parents and children to forgo COPPA's protection and take greater risks in order to get access to the educational and communication sites they want to be part of their online experiences.²⁷

The FTC's proposed changes, however, do not address these fundamental challenges because the proposed changes to the Rule are focused on child-directed sites and do not help resolve the ambiguity surrounding online destinations that are frequented by children. Thus, the amended COPPA Rule does not change, increase, or encourage the implementation of further privacy protections by such sites and services, so long as they lack actual knowledge that users are children. Additionally, the FTC's proposed changes to the Rule create new restrictions for websites and online services that are construed as directed to children, which are likely to drive even more operators of websites and online services to forgo investing in family-friendly content and services, and instead focus on controls to avoid knowledge that a user is a child, or to restrict its users to those over 12 years. Panelists in the FTC COPPA Rule Review Roundtables in 2010 discussed the need to avoid perpetuating such "reverse incentives" for operators and, instead, find new ways to engage them in adopting privacy protections.²⁸

Separately, the Commission's proposed changes to the COPPA Rule also may have the unintended consequence of making it more difficult for operators to provide children with rich interactive services directed to them because the Commission's proposal is overly restrictive on the type of data that can be collected to provide basic website or online service functionality. For example, the proposed exception under "*support for the internal operations of the website or online service*" relating to technical support raises concerns because the limitation for technical support does not clearly encompass actions and use of information necessary to provide a positive interactive user experience. Similarly, the proposed broadening of the "*personal information*" definition to include "persistent identifier" will restrict the ability of websites and online services to deliver the desired personalized and optimized content and services expected and demanded by users through the use of first-party cookies, including, for example, providing direct access to a favorite game or feature on the homepage (rather than forcing the user to click through the website on each visit to find the preferred game, service or activity).

Further, the proposed change to include "*screen or user name*" within the definition of "*personal information*," if used other than for supporting the internal operations of the website or online service, may be read to restrict or eliminate certain popular website features that involve the use of an anonymous screen or user name. This interpretation of the proposed change to the Rule is the case even when the screen or user name is not associated with any personal information and does not allow for the user to be directly contacted online by anyone. The proposed change to screen or user name also may be read to restrict the use of a single screen or

²⁷ *Id.* at p. 23.

²⁸ See Comments of Jeffrey Greenbaum, FTC COPPA Rule Review Roundtables transcript at p. 91 (June 2, 2010).

user name on the same website or online service, but which is made available on different platforms.

In sum, while just a few years ago in its 2007 report to Congress, the FTC concluded that the COPPA Rule did not adversely affect “the number of websites directed to children or the ability of children to access online information of their choice,”²⁹ the same can not be said about the outcome with the FTC’s current proposed changes to the COPPA Rule given what we now know about the way that children and families use the Internet. The current proposed changes and resulting unintended consequences would further restrict information collection and use (and thereby stifle innovation and the delivery of content and interactive services that engage users of all ages). This, as a result, will drive children to more sites and online services that are not designed and intended to be used by them, and which lack the types of privacy controls that are on sites and services that are designed for and directed to children. The more restrictive Rule is also likely to dampen incentives for the creation of online services intended for all audiences — children, teens and adults alike — by increasing the risk of being construed as sites or services “directed to children” under the revised Rule.

Thus, the end result of the proposed changes is likely to be an outcome that would undermine two key objectives of the COPPA Rule: (1) placing parents “in control of the online collection and use of personal information from their children,”³⁰ and (2) minimizing the burden on operators that provide interactive online content for children.³¹

II. A Refined Approach Would Foster Privacy Protections and Family-Friendly Content on More Websites and Online Services Used by Children than the Current COPPA Framework

Industry and the Commission should collaborate to address these serious public policy challenges in ways that encourage privacy safeguards and parental controls on the use of children’s information on websites and online services in a manner that facilitates the development and delivery of innovative, interactive online content and services that are enjoyed by users of all ages. To that end, Disney proposes that the Commission recognize an additional classification of websites and online services that will (a) foster an environment where online operators are encouraged to construct and operate websites and online services “directed to children” and (b) contribute to the development of family-friendly websites and online services that achieve COPPA’s essential goals by embracing the Rule’s data minimization, transparency, and parental consent-based privacy protections. The FTC could accomplish this end by providing a clear path for operators of “family-friendly” websites and online services to be assured that they are in compliance with COPPA without having to treat all users of the site and service as though they are children. The Commission could create this path by clarifying within the COPPA Rule that a website or online service that includes family-friendly content attractive to users of all ages, and protects the privacy interests of children who access the site or service in

²⁹ FTC Report to Congress (Feb. 2007) at p. 2.

³⁰ Pitofsky (Sept. 23, 1998).

³¹ J. Rich (Apr. 29, 2010).

a manner that is consistent with the COPPA goals, but does not treat all users as though they are children, would not be in violation of COPPA.

To qualify under this clarification, such family-friendly websites and online services would have to satisfy robust privacy protections that would extend *to all users*, as well as satisfy COPPA's statutory and implementing regulatory requirement that makes it "unlawful for an operator of a website or online service directed to children ... to collect personal information *from a child*"³² without first obtaining verifiable parental consent, thereby exceeding the protections generally extended by general audience websites. In direct recognition of the fact that children are some of the users of these sites, the relevant rules would be designed specifically to determine which users are children before any personal information is collected. When the operator determines a user is a child, the COPPA requirements for treatment of children would then be triggered and applied. However, in direct recognition that the website or online service is designed to span family demographics, unlike for websites and online services directed to children, not all users would be presumed to be children. Rather, these websites and online services would be required to be designed deliberately to avoid the collection of personal information until age of the user is ascertained.

Specifically, under the family-friendly framework recommended by Disney, the FTC could specify a series of requirements that are consistent with COPPA's privacy objectives. For example, first, the operator of a family-friendly website or online service would be required to establish age prior to the collection of personal information³³ from any user in order to obtain the appropriate parental permissions. Prior to the collection of personal information, an operator would be required to request the user's age using an approach that is consistent with current guidance on the proper implementation of age verification questions.³⁴ In instances where the user is identified as being under 13, the operator would then be required to provide an age appropriate experience by either avoiding the collection of personal information for these children, or by providing notice to the child's parent and obtaining affirmative verifiable consent for the collection of the child's personal information in a manner consistent with the COPPA Rule requirements.

Second, the operator would be required to take reasonable measures to delete personal information from postings (*e.g.*, through moderated or filtered chat) within the website or online service to prevent the disclosure of personal information by children under age 13. The operator

³² The Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, at Sec. 1303(a)(1)(emphasis added).

³³ As discussed in greater detail in Section V(B) and (C) below, irrespective of the Commission's decision on whether to adopt the family-friendly website or online service distinction, Disney urges the Commission to modify the definition of "personal information" and "screen or user name" under the proposed changes to the COPPA Rule to exclude first-party tracking of a persistent identifier, and allow screen or user names to be used for participating in interactive website features and to access more than a single website or online service.

³⁴ See TRUSTe, *Complying with COPPA, TRUSTe's Guidelines for General Audience Websites* at 2-3, available at http://www.truste.org/docs/How_to_Comply_with_COPPA.doc.

would be excluded from the moderator requirement only in instances where the operator has actual knowledge that the user of the chat feature is 13 or older.

Third, unless the operator had actual knowledge the user is a child, the operator would not be required to obtain prior parental consent for passive tracking through a persistent identifier on a family-friendly site or online service, and this exception would only apply to those family-friendly websites or online services that meet certain well-defined conditions designed to enhance opportunities for parental control, such as:

- The website or online service provides a clear and prominent opportunity throughout the website and online service for users, including parents, to opt-out of passive tracking by third-party advertisers;
- The website or online service adheres to the Digital Advertising Alliance’s (“DAA’s”) Self-Regulatory Principles for Online Behavioral Advertising.³⁵ Among other terms, these self-regulatory principles provide for ad-based enhanced notice and control opportunities, and do not permit behaviorally targeted advertising directed to children without parental consent;
- The website or online service does not sell or rent children’s personal information, including geolocational data, to third parties without obtaining prior affirmative parental consent.

The following chart helps illustrate how this family-friendly framework would extend and encourage more robust privacy protections, including data minimization, transparency and parental controls, by operators of the different kinds of websites and online services with which children are engaging.

Rules by Type of Website / Online Service

			General Audience
Collection of Personal Information (“PI”)	<ul style="list-style-type: none"> • No collection of children’s PI without prior verifiable parental consent 	<ul style="list-style-type: none"> • Must verify age before collection of PI and obtain verifiable parental consent where user is under age 13 • Take reasonable measures to prevent the disclosure of PI (e.g., through moderated or filtered chat) unless operator has actual knowledge user is an adult 	<ul style="list-style-type: none"> • Collect PI without parental permission or asking age • Moderation of chat is not required

³⁵ See Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), available at www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

Passive Tracking	<ul style="list-style-type: none"> • No passive tracking without verifiable parental consent 	<ul style="list-style-type: none"> • Except where the operator has actual knowledge the user is a child, limited exception to consent rule for passive tracking, only if: <ul style="list-style-type: none"> ○ website provides prominent opt-out opportunity ○ Adherence to DAA Principles for Online Behavioral Advertising ○ Does not disclose PI without affirmative parental consent ○ Passive tracking cannot be used for behavioral ads targeted to children, per DAA requirements • Where the operator has actual knowledge the user is a child, no passive tracking without verifiable parental consent 	<ul style="list-style-type: none"> • Allowed for any purpose • No enhanced control options required • Adherence to DAA Principles for Online Behavioral Advertising not required
Precise Location	<ul style="list-style-type: none"> • No collection of precise geolocation information without parental permission 	<ul style="list-style-type: none"> • No collection of precise geolocation information without parental permission 	<ul style="list-style-type: none"> • No restrictions on collection of precise geolocation information

The family-friendly framework proposed by Disney would directly address the public policy challenges confronting all parties affected by the current COPPA framework. Specifically, the approach ensures that there is no dilution of any existing COPPA requirements. That is, where the operator of a family-friendly website or online service is interacting with a user under the age of 13, it must comply with all applicable Rule provisions. But the family-friendly framework encourages enhanced child-sensitive and protective privacy measures by operators of the many sites and online services that are popular with children. The family-friendly framework thus would promote data minimization by restricting the collection of children’s personal information unless obtained with verifiable parental consent, and increase transparency and parental control on such sites by requiring that parental choice mechanisms appear in a prominent, relevant, and easily accessible location on the website or online service. In this way, the framework would give fuller meaning to the privacy protections intended by COPPA by reaching children wherever they are on the Internet. At the same time, by creating greater certainty that doing so would not run afoul of COPPA, this would encourage a larger number and more diverse scope of companies and online platforms to participate in the creation

of family-friendly sites and online services, and embrace principles of parental engagement and privacy by design.

In particular, the proposed framework would facilitate and encourage operators to develop and deliver more online content and services that are family friendly, which directly supports the Commission’s objective of “maintaining children’s access to the Internet, preserving the interactivity of the medium, and minimizing the potential burdens of compliance on companies, parents, and children.”³⁶ The proposed framework would fulfill these objectives by providing a rational path for the development of family-friendly, privacy-protective Internet content and services, which would in turn encourage greater investment in family-friendly services such as premium content incorporated into a family-oriented service. The resulting increase in family-friendly options would provide greater privacy protection to children by giving them more appropriate online outlets than are available today.

Thus, by adopting a new family-friendly option for COPPA compliance, the Commission would provide needed compliance flexibility to encourage a range of business models under which companies could offer valuable interactive content to users of various ages, while at the same time ensuring that children are afforded the privacy protections demanded by COPPA, regardless of the path pursued by the operator. Importantly, however, this proposal would not dispense with the need for rules for website and other online services directed to children where it is appropriate to treat all users as children. For example, some operators may develop a value proposition for a service directed to children, obtain verifiable parental consent at the outset and collect personal information consistent with that consent. Others may choose to develop a family-focused experience and invest in the ability to provide an age differentiated experience that purposefully treats users of various ages differently. Indeed, a new class of websites and services likely some of which today operate as general audience websites, would take advantage of the new opportunity and invest in the creation of family-friendly experiences embracing principles of data minimization, parental control and transparency. The end result, from a public policy perspective, is that children would not be subject to data collection without parental permission and a greater number of websites and online services would incorporate measures that are protective of children’s privacy.

III. Proposed Implementation Approaches for a “Family-Friendly” Framework

The family-friendly framework recommended by Disney would represent a new approach that would advance the COPPA Rule’s principal objectives. As such, Disney respectfully recommends three potential options to implement the framework pursuant to the Commission’s existing authority under the COPPA statute.

³⁶ Children’s Online Privacy Protection Rule; Final Rule, 64 Fed. Reg. 59804, 59889 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312).

A. Clarify A “Family-Friendly” Exclusion Within the COPPA Rule’s Definition of a “Website or Online Service Directed to Children”

As noted previously, many operators struggle with determining whether their website or online service is, in fact, “directed to children” because the site or online service includes one or more of the factors under the COPPA Rule’s “totality of factors” test.³⁷ One way that operators take steps to be confident that they are in compliance with COPPA is to make changes to their site or online service to ensure that it will not be construed as one that is “directed to children” by eliminating from their site or online service some or all of the factors that are part of the Rule’s “totality of factors” test. Because this manner of complying with COPPA (a) deters the creation of family-friendly websites and online services, and (b) does not embrace the privacy protections intended by COPPA on these sites and online services even when children use them, Disney believes that the Commission should implement a family-friendly framework by clarifying within the COPPA Rule that a “family-friendly” website or online service falls within an express exclusion from the definition of a “*website or online service directed to children.*”

The Commission could provide this clarification through its discretion under COPPA by inserting a narrowly-drawn family-friendly distinction into the current definition of “*website or online service directed to children*” that would mandate the framework’s requirements as detailed *supra* in Section II of these Comments. The Commission is well-situated to create such a distinction within the COPPA Rule definitions, as the proposed clarification is supported both by the Act and by precedent where the FTC has instituted carve-outs from regulatory definitions or new requirements within other FTC rules, even where such distinctions were not expressly called for in the implementing statute.

For example, in the current COPPA Rule, the definition of “website or online service directed to children” already provides a clarification of what would not be considered such a website or online service. The Rule provides that “a commercial website or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a director, index, reference, pointer, or hypertext link.”³⁸ The family-friendly framework proposed by Disney could be added to this existing exception within the definition of a “website or online service directed to children.”

Similar examples are present in other FTC Rules. For example, the FTC instituted changes within the Telemarketing Sales Rule (“TSR”),³⁹ which are particularly instructive and

³⁷ Children’s Online Privacy Protection Rule, 16 CFR 312.2 (within the definition of “website or online service directed to children,” the Rule provides that “*In determining whether a commercial website or online service, or a portion thereof, is targeted to children, the Commission will consider the subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities.*”)(current, non-amended version).

³⁸ *Id.*

³⁹ Telemarketing Sales Rule, 16 C.F.R. Part 310.

provide an appropriate guide for the proposed revision to the COPPA Rule. The changes to the then-existing TSR Rule, which the FTC believed were necessary to achieve the consumer protection objectives of the TSR, were not based on express language within the implementing statute,⁴⁰ but were made pursuant to the Commission’s authority to “prescribe rules prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices.”⁴¹

These include, for example, in 2002, the Commission instituted the national “Do Not Call” (“DNC”) registry.⁴² Despite a legal challenge to the FTC’s authority to create the registry, the Tenth Circuit held that the FTC’s conclusion that it had authority under the Telemarketing Act to enact the registry was a permissible construction of the statute and was entitled to deference.⁴³ The FTC also created a carve-out provision in the TSR by instituting the established business relationship (“EBR”) exception, even though the implementing statute did not provide for such an exception. The exception was instituted by the FTC to avoid detrimental effects to merchants who would be unable to place phone calls to customers with whom they had engaged in a recent transaction.⁴⁴ The FTC reasoned that the EBR exception was “consistent with consumer expectations” and was acceptable as long as it was “narrowly tailored and clearly defined to avoid a loophole that could defeat the purpose of the national do-not-call registry.”⁴⁵

The COPPA statute presents the Commission with a similar opportunity to enhance the COPPA Rule to better protect children while encouraging innovation. And like the EBR exception in the TSR Rule, the family-friendly framework proposed by Disney is wholly consistent with consumer expectations, particularly given the increasingly multigenerational online viewing patterns and parents’ interest in maintaining some form of control over their children’s online experiences on the websites and online services their children use, while also not requiring that all the adult users on a family-friendly site be treated as a child for COPPA purposes. The proposed clarification that the family-friendly category be excluded from the definition of a “website or online service directed to children” can be narrowly-crafted and clearly defined to both align with consumer expectations and fulfill the privacy objectives of the COPPA Rule.

Indeed, in many respects, the Commission’s recognition of the appropriateness of an “age gate” for “teen-directed” websites (*i.e.*, an age verification question that blocks users under 13

⁴⁰ Telemarketing and Consumer Fraud and Abuse Prevention Act (“Telemarketing Act”), 15 U.S.C. § 6101.

⁴¹ Pub. L. 103-297, 108 Stat. 1545 §3.

⁴² 16 C.F.R. § 310.4(b)(ii)(B).

⁴³ *Mainstream Marketing Services, Inc. v. FTC*, 358 F.3d 1228, 1250 (2004); the FTC’s Established Business Relationship Rule was not challenged, although the 10th Circuit did address the FCC’s creation of a similar Established Business Relationship Rule as used within the Telephone Consumer Protection Act, finding it was an appropriate use of the agency’s discretion in furthering the intent of the statute.

⁴⁴ 16 C.F.R. §310.4(b)(iii)(B)(ii).

⁴⁵ Telemarketing Sales Rule, 68 Fed. Reg. 4591 (Jan. 29, 2003).

from using the site), as reflected in the FTC’s COPPA “Frequently Asked Questions,”⁴⁶ demonstrates that the discretion to define websites and online services “directed to children” can include an exclusion for a new category (teen-directed) so long as it includes appropriate protections for children (an age gate). Further, the COPPA Rule provides other exceptions that are not expressly called for in the statute, but nevertheless were instituted by the FTC after weighing factors including cost, the desired child privacy protections, and available technology. For example, the COPPA statute does not distinguish between external and internal uses of personal information, yet the COPPA Rule adopted a sliding scale approach whereby an operator, when collecting personal information only for its internal use, may obtain verifiable parental consent through an email from the parent, so long as the email is coupled with an additional step (the “email plus” method). Notably, the Commission instituted the sliding scale approach after it was “persuaded by commenters’ views that internal uses of information, such as marketing to children, presented less risk than external disclosures of the information to third parties or through public postings.”⁴⁷ Such past actions by the Commission with respect to COPPA provide the appropriate basis under which the Commission can implement the family-friendly framework proposed by Disney.

History supports the FTC’s use of its discretion to provide clarification of specific practices or types of entities that do not fall within a regulatory definition, even where such exceptions were not expressly authorized by the implementing statute but, nevertheless, were deemed by the Commission to be necessary and appropriate to accomplish the statutory mandate in light of dynamics occurring within the environment in which the rule operates.⁴⁸ As we have described, a clarification that provides for a family-friendly, narrowly-crafted exception within the definition of “website or online service directed to children” will position the COPPA Rule to respond more effectively to the present and still-changing online environment for the reasons described above.

B. Safe Harbor for Family-Friendly Websites and Online Services

As an alternative to the definitional approach within the COPPA Rule discussed above, Disney respectfully requests that the Commission consider supporting and encouraging submissions for a safe harbor proposal based on Disney’s proposed family-friendly framework. The FTC has long recognized that industry self-regulation “can respond more quickly and flexibly than traditional statutory regulation to consumer needs, industry needs, and a dynamic marketplace.”⁴⁹ Moreover, the FTC has previously stated that it prefers self-regulation instead of a detailed legislative mandate “because of the rapidly evolving nature of the Internet and

⁴⁶ See FTC, *Frequently Asked Questions about the Children's Online Privacy Protection Rule* at Q. 39, available at <http://www.ftc.gov/privacy/coppafaqs.shtm>

⁴⁷ 76 Fed. Reg. 59819 (Sept. 27, 2011) at n.147.

⁴⁸ In addition to the examples provided, see the Comprehensive Smokeless Tobacco Health Education Act (16 C.F.R. §307.4(b)) (exempts certain advertising from ban on advertising; *see also* the Textile Fiber Products Identification Act (16 C.F.R. §303.43) (provides a due care exception for certain misbranded products).

⁴⁹ FTC Report to Congress, *Implementing the Children’s Online Privacy Protection Act* (Feb. 2007) at p. 22.

computer technology.”⁵⁰ As discussed, given the increasing use of the Internet by children and the speed with which new and highly-interactive online platforms are being introduced into the market, a safe harbor based on the family-friendly framework merits strong consideration.

The COPPA statute allows the FTC to establish a safe harbor for participants in FTC-approved, COPPA self-regulatory programs. To be approved, among other requirements, the self-regulatory program must contain guidelines that protect children’s online privacy to the same or greater extent as the COPPA Rule and ensure that each potential participant complies with the guidelines. Disney’s proposed family-friendly category of websites and online services and corresponding obligations would achieve the requirements for a safe harbor, and would protect children’s online privacy *to a greater extent* than under the COPPA Rule for multiple reasons.

First, if a family-friendly website or online service has actual knowledge that it is collecting a child’s information, it must comply with the Rule’s requirements accordingly. In this way, the family-friendly safe harbor would not permit a work-around of COPPA privacy protections. Rather, the safe harbor could extend privacy protections to more websites and online services than are currently covered by the Rule because the websites and online services lack actual knowledge that some users are children. These additional privacy protections include establishing age prior to the collection of personal information from any user in order to obtain the appropriate parental permissions, and moderating online chat features by all users unless the operator has actual knowledge the user is an adult to prevent the disclosure of personal information—a privacy safeguard that is not required or provided even by many child-directed sites, and thus would protect children’s online privacy to a greater extent than under the COPPA Rule.

Further, a family-friendly website or online service would not sell or rent children’s personal information to third parties unless it had obtained prior affirmative parental consent to do so, would be restricted from using information collected through third-party cookies to deliver behaviorally-targeted advertising unless it provides a clear and prominent opportunity throughout the website or online service for users, including parents, to opt-out of passive tracking by third-party advertisers, and would need to adhere to the Digital Advertising Alliance’s (“DAA’s”) Self-Regulatory Principles for Online Behavioral Advertising, which provide ad-based enhanced notice and control opportunities and do not permit behaviorally targeted advertising directed to children without parental consent. These restrictions on use of third-party cookies also would protect children’s online privacy to a greater extent than under the COPPA Rule.

In sum, these safeguards are far more robust and protective of privacy than what is done currently by many general audience websites and online services that children frequent. Further, because the family-friendly safe harbor would provide greater certainty of COPPA compliance, it would be an attractive option for general audience sites and online services that children are using and will continue to use. At the same time, it would encourage such operators to invest in responsible privacy practices and safeguards, and to create more content and services that are

⁵⁰ Pitofsky (Jul. 21, 1998).

intended for users of all ages, including families. Disney therefore seeks the Commission’s support for a new safe harbor category based on the family-friendly framework.

C. Advisory Opinion that Distinguishes a “Family-Friendly” Website from a “Website Directed to Children”

As an additional alternative to the above-stated proposals, Disney requests that the FTC issue an advisory opinion that would clarify that a family-friendly website or online service is not a “website directed to children” in instances where the website or online service meets the criteria and safeguards described above.

The Commission will consider a request for an advisory opinion in instances where (1) the matter involves a substantial or novel question of fact or law and there is no clear Commission precedent; or (2) the subject matter of the request is of significant public interest.⁵¹ A request for the Commission’s clarification on the family-friendly framework would meet both of these requirements. Specifically, the family-friendly framework is a new proposal that is not currently addressed in the COPPA Rule. However, its adoption or endorsement by the Commission would have significant implications for online operators that offer content that is attractive to a multigenerational audience. Further, as discussed above, consumer involvement in the online environment continues to expand and there is significant public interest in identifying new approaches through which a broader base of online operators can embrace principles of parental engagement and invest in privacy protections for children.

IV. A Cooperative Consent Mechanism May Enhance Parental Verification Efforts

As discussed above, children increasingly are accessing websites and online services through web-based platforms and other online portals that involve collaboration between operators, carriers, manufacturers, developers and service providers. This shift away from direct access to each individual website and online service necessitates the creation of new parental outreach and consent mechanisms that leverage these cooperative service delivery technologies to offer prominent and convenient verification mechanisms that will increase transparency. At the same time, these new technologies create opportunities for improved platform-based parental controls.⁵²

The lack of effective verification methods to determine a child’s age and identify parental relationships remains a vexing public policy challenge and acts as a barrier to broader implementation of COPPA. Parents, children, the online industry, and the Commission have an equally vested interest in this topic, and developing solutions that are appropriate for the online platform environment will require sustained cooperative action. The Commission is in the

⁵¹ 16 C.F.R. § 1.1(a)(2).

⁵² For instance, CTIA, the wireless industry trade association, recently announced the creation of a mobile application rating system that ultimately will lead to member storefronts offering new tools that will provide parents with greater transparency as to the data collection practices of mobile applications and greater ability to control the applications children can access. *See* www.ctia.org/media/press/body.cfm.prid/2147.

unique position to stimulate dialogue and encourage the industry action that is necessary to shift from the present verification model — which requires outreach by each individual website, online service, and platform — to a more streamlined, contextual approach that can better achieve the privacy objectives of COPPA as young children continue to expand their online footprint.

One practical approach to verification that is well-suited to the web-based platform environment would involve creating a simple ecosystem solution — a “Kids Privacy Portal” — through which parents can express privacy preferences in one place for multiple online activities. Participating operators would agree to abide by the privacy permissions established by the parent, providing parents with a one-stop control center.

A Kids Privacy Portal solution would allow parents to grant permission for their child to participate in an online service that intends to collect personal information from their child. Parents could obtain a username and password that allows them to register directly on the centralized portal, or through a corresponding mobile application, to input their consent preferences for multiple online destinations that may be of interest to their child. The parent also could be prompted to visit the portal or mobile application by an operator seeking permission in relation to its website or online services. The parent would need only his or her username and password to later modify or update the consent preferences, and the updates would occur in real-time. Such a solution would be developed in a manner so that operators could rely on this authentication as COPPA-compliant verifiable parental consent. As an additional feature (not required by COPPA), the portal solution could, through appropriate interfaces with member companies, enable parents to log-in to the solution to generate an aggregated view or report of their consent activities over time and make modifications that they feel are appropriate.⁵³

Another possible approach would allow a platform operator to obtain verifiable parental consent on behalf of application providers under a joint agreement that determines how data will be collected and used, and how parents exercise control. Under this approach, the platform could acquire parent contact information and obtain verifiable parental consent after providing parents with the required notice on behalf of the operators who agree to collect, use, and disclose children’s personal information only in the manner described in the notice. Operators interested in additional collection or use would have to provide parents with a separate notice and obtain additional verifiable parental consent that covers such further collection, use, or disclosure of the child’s information. Also, a platform provider potentially could leverage its platform to provide parents with new just-in-time transparency and control features, such as real-time notice on when and how a child is using an application, that go well beyond the one-time consent model of COPPA. Such an approach could significantly improve parental control.

Disney recognizes that implementing joint approaches to consent would require extensive collaboration and cooperation among all key stakeholders. An ecosystem solution, however, would yield a number of benefits. It would address the Commission’s concern over the lack of innovation with respect to verification methods by offering users an approach that is consistent

⁵³ Such a mechanism could also be expanded to include other functionality that may be of interest to parents, including controls for access to age-restricted services, or interaction with age-rated services.

with other meaningful choice mechanisms supported by the Commission (including the Commission's support of a single, easy to use, universal, and persistent Do Not Track mechanism). Moreover, a portal or cooperative consent solution would more strongly engage parents by providing an efficient, streamlined mechanism enabling greater control and visibility into their child's online activities.

As such, we strongly urge the Commission to exercise its leadership on this issue and encourage operators to develop such approaches. We believe the Commission can play an important role in encouraging industry to innovate in this area by developing baseline criteria for the creation of a cooperative verification mechanism that would comply with COPPA. The Commission also could solicit input on improved parental controls, convene stakeholders to address any technological barriers, and facilitate greater innovation on this issue. The ultimate objective of the Commission's efforts would be to encourage adoption of cooperative consent mechanisms that comply with the Commission's rules, promote COPPA's goals of empowering parents to become more active in their children's online activities, and provide sufficient flexibility for companies to develop robust interactive experiences in which children can participate in safe and secure ways.

V. Proposed Definitions of “Personal Information” and “Support for Internal Operations” Are Too Restrictive to Provide Robust Interactive Services

A. “Support for Internal Operations” Definition Should Encompass Use of Persistent Identifier Information to Improve Site and Service Functionality and Enhance the User Experience Through Greater Personalization

In the proposed changes to the COPPA Rule, the FTC recognizes that the definition for “support for the internal operations of the website or online service” is intended to be a limiting term that would exclude data that is collected under this definition from triggering COPPA's “disclose or disclosure” defined term, or “screen or user name” or “persistent identifier” terms within the definition of “personal information” (and thus exclude the verifiable parental consent requirement).

The FTC's proposed definition of “support for the internal operations of the website or online service” provides that the term, in part, “means those activities necessary to maintain the technical functioning of the website or online service.” The Commission's comments further explain that “operators use persistent identifiers and screen names to aid the functionality and technical stability of websites and online services and *to provide a good user experience*, and that the Commission did not intend to limit operators' ability to collect such information from children for these purposes.”⁵⁴

Disney respects that the Commission is mindful of allowing a single website or online service to continue to collect persistent identifiers without verifiable parental consent if such information is used to aid the functionality and technical stability of the website or online service

⁵⁴ Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59809-59810 (Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312).

and to provide a good user experience. Disney, however, respectfully notes that to actually achieve these goals and to have the ability to personalize the online experience and to develop and foster dynamic, interesting online content that engages children, it is critical that a company be able to collect and analyze persistent identifier information, and that this information can be collected and analyzed without interfering with privacy protections. Disney therefore requests that the Commission clarify the definition of “support for internal operations” so that it expressly incorporates usage of persistent identifier information to improve site and service functionality and user experience.

B. The COPPA Rule Should Permit Reasonable Use of Persistent Identifiers Consistent with Self-Regulatory and FTC Policy on First-Party Use of Such Information

Companies that provide content or service online may do so through a single online destination, or they may offer multiple web-based channels that are intended to appeal to a range of audiences. Such companies that have invested in creating online platforms that offer a range of content should not be precluded from offering users a unified, personalized experience across these multiple services. This is particularly true — and consistent with privacy objectives — when the only identifier used for such purposes is a persistent identifier that is not linked to personal information and is not used for third-party online behavioral advertising directed to children.

The Commission’s proposed changes to include “persistent identifier” within the “personal information” definition *if used other than/or in addition to “support for internal operations of ... the website or online service,”* and to expand the definition of “personal information” to include identifiers that link the activities of a child across different websites or online services, means that a company, irrespective of the privacy protections incorporated into its site, may no longer be able to provide a user with personalized, optimized content or through multiple centrally-controlled websites or online services unless the operator collects more (not less) personal information, and obtains verifiable parental consent. This type of restriction is not beneficial to consumers because it will inevitably reduce the amount of personalized online content and feature-rich functionality developed for children and families, and stifle innovation.

A more practical and, therefore, preferable approach is to keep the COPPA Rule revisions consistent with self-regulatory and FTC policy statements concerning first-party use of persistent identifier information, which recognize that first-party data collection and use is within consumers’ reasonable expectations and is therefore permissible.⁵⁵ This approach would promote better understanding and compliance by industry as to the acceptable use of persistent identifier information, including within the area of online behavioral advertising. In contrast, prohibiting the use of persistent identifiers under COPPA (even if not associated with any personal information and not used to direct behavioral advertising to children), in contrast to the DAA’s self-regulatory principles and the Commission’s other statements regarding first-party

⁵⁵ See, e.g., Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), available at www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 2010); FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009).

use of persistent identifier information may create confusion by consumers and businesses and lead to inconsistent compliance and further unintended adverse consequences in the marketplace.

In addition, as a practical matter, if collection of a persistent identifier alone triggers collection of children’s personal information under COPPA, it is unclear how a company would be able to comply with the Rule, given that a persistent identifier is collected at the initial point of visitation — when the operator of a general audience website likely would not know if the user is a child or, if it later discovers that the visitor is a child, would face challenges in identifying and deleting persistent identifiers stored and amassed elsewhere if disassociated with any personal information. Panelists at the FTC’s COPPA Rule Review Roundtable in 2010 discussed how expanding the scope of “personal information” to include certain persistent identifiers would actually force operators to collect *more* personal information prior to obtaining verifiable parental consent since IP addresses alone, for example, would not provide the operator with sufficient data to contact a parent.⁵⁶

Therefore, Disney recommends modifications to the Commission’s proposed definitions of “*personal information*” and “*support for the internal operations of the website or online service*” to allow for reasonable first-party use of persistent identifiers that will enable operators to create a personalized, optimized experience. Further, Disney recommends that the Commission modify the definition of “personal information” so that a single business entity will not be precluded from creating a more unified online experience across its multiple online outlets based on first-party use of persistent identifiers.

C. The Commission’s Proposed Change to “Screen or User Name” within the Definition of “Personal Information” Should Not Be Adopted as Proposed

Screen or user names are widely used in the online environment and provide the most effective tool available for operators to allow sign-on to (1) a single website; (2) a single online service that runs on multiple platforms; (3) multiple distinct websites or online services controlled by a single operator; and (4) interactive online features, such as moderated chat functionality within an online game, or for a user to post an anonymous “shout out” message on a website or online service. Moreover, screen names can be a significant contributor to an operator’s consumer data minimization strategy by eliminating the need to collect personal information before allowing access to the interactive features of an online destination.

The Commission’s proposed change in the COPPA Rule to include “screen or user name” within the “personal information” definition *if used other than/or in addition to “support for internal operations of ... the website or online service,”* can be read to mean that a company would be unable to allow a single screen or user name to be used across more than a single website or online service, or potentially for the same service across different platforms, including

⁵⁶ FTC COPPA Rule Review Roundtable transcript, comments of panelist Sheila A. Millar at p. 185-86 (June 2, 2010) (“If suddenly those items are personal information, plus the IP address, you undercut this assumption of how you provide a pretty anonymous experience to a child and you force the website to turn to a more privacy-invasive model, perhaps, because you have to collect more personal information. The IP address alone will not allow that website to contact the parent and to get parental consent . . .”).

for basic functionality, such as pausing a game that was initiated on one platform (online) and continuing it on a different platform (mobile application). Also, the proposed change is unclear even with respect to the use of screen or user names within a single website. For example, the text of the Commission’s proposal states that screen names may be used “to identify users to each other,” such as within a chat feature that is part of an online game;⁵⁷ however, the proposed revised Rule may be interpreted as precluding this type of screen name use. Similarly, popular interactive features, such as leaderboards for online games or applications that enable “shout outs” to other site users, rely on screen names to maintain user anonymity, and without allowing anyone to directly contact that user. Based on the proposed revised Rule, it is unclear whether use of screen names for these purposes would be permitted.

The Commission explains that its proposed expansion of the term is necessary based on the assumption that, if a screen or user name can be portable across multiple websites or online services, then the screen or user name would permit the direct contact of a specific individual online.⁵⁸ This nexus is required by COPPA, given that the definition of “online contact information,” by statute, can only include an identifier “that permits the direct contact with a person online.”⁵⁹ The Commission’s characterization that a screen or user name, in fact, permits the direct contacting of a child online, however, is not supported by any evidence or analysis that details the scope of the perceived public policy concern or indicates how a person necessarily can be directly contacted based on their screen name. Nor does it acknowledge the range of appropriate circumstances in which screen or user names are used. While screen or user names can be used to access basic site functionality on one or sometimes multiple online services, or perhaps a single service on multiple platforms — which facilitates and encourages children to continue to explore and interact with appropriate websites and online services — this does not present the ability for others to directly contact the child.

For these reasons, the Commission’s proposed change is overly broad and could result in new, unnecessary burdens for children who could be restricted from certain popular website features and may discourage operators from providing interactive online content even when such content does not involve personal information or permit the direct contacting of a child. Additionally, parents would now have to provide verifiable parental consent on each website or online service (and for each platform that the website or online service is made available, such as website, console, and/or mobile), even when the parent is comfortable with the privacy practices of the operator (regardless of platform in which the service is used), and again even where the screen or user name does not permit the direct contacting of the child.

Precautions can be taken in the design and use of the screen name to address the concerns raised by the Commission and still allow the screen name to be used to participate in popular chat and interactive website features, and to access more than a single website or online service, or the same website and online service that is available on more than one platform.⁶⁰ And if such

⁵⁷ Children’s Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59810 (Sept. 27, 2011).

⁵⁸ *Id.*

⁵⁹ The Children’s Online Privacy Protection Act of 1998, Pub. L. 105-277, at Sec. 1302(12).

⁶⁰ For example, the screen name creation feature can (1) require special character and number combinations to inhibit the use of real names; and (2) include prominently-placed statements/warnings

precautions can be taken, there is limited reason to encompass the term within the broad definition of “personal information” as currently proposed, and subject the collection of the screen or user name to verifiable parental consent requirements.

The consequence of triggering prior verifiable parental consent before collecting user name information will create unnecessary challenges and obstacles that could discourage the development of child-directed and family-friendly sites. For example, some child-directed websites and online services available today are designed not to collect any personal information from children, but which provide interactivity through the use of anonymous user and screen names. The benefits of this feature include allowing children to immediately access interactive content upon their visit to the website or online service, without first requiring the child’s parent to complete the verifiable parental consent process. If obtaining verifiable parental consent were to be required in order for an operator to provide such an interactive experience, this additional step — and resulting burden on the operator, parent, and child, and delay in the child’s ability to access the interactive feature — may deter operators from developing and providing such features, and deter children from accessing such child-directed and family-friendly websites and online services with privacy controls. And if the availability of interactive options decreases on child-directed and family-friendly online destinations, children are more likely to forego such destinations, and instead explore general audience websites and online services that do not invest in similar privacy protections.

Another consequence of requiring prior verifiable parental consent before collecting user name information ironically may result in an *increase* in the collection and disclosure of children’s personal information. For example, operators that currently moderate user and screen names on child-directed and family-friendly websites and online services to ensure that they do not include personal information may conclude that the expense of moderating the site or online service is unwarranted. Rather, the focus by such operators could simply shift to obtaining verifiable parental consent, which, if the parent provides consent to collect and disclose the child’s personal information, would result in an increase of children’s user and screen names that contain personal information. This result would run counter to the data minimization principles of COPPA.

Balance is critical in this area. Given the many safeguards readily available to address the Commission’s stated concerns regarding screen and user names, and the many benefits that result from a framework that encourages the use of privacy-protective anonymous screen and user names without first obtaining verifiable parental consent, we recommend that the Commission reconsider or further qualify how it has currently positioned the term “screen or user name” within the definition of “personal information.”

* * * * *

Ongoing changes with respect to the manner and extent to which children now interact on the Internet require that industry and the Commission continue to reexamine existing online

that users should avoid real names, and to avoid using the same screen or user name on different websites and online services.

privacy protections, as well as identify and implement new solutions. Disney greatly appreciates the Commission's efforts to see that children can leverage increasingly interactive online content in a safe environment. Disney recommends that the Commission consider a new framework that will create the necessary incentives for a larger share and more diverse scope of businesses to embrace robust privacy protections, including transparency and parental controls. Disney also recommends that the Commission use its leadership position to foster continued dialogue between industry and consumers on new parental verification mechanisms that can leverage current and evolving platform technologies to improve transparency and parental control. Lastly, Disney recommends that the Commission clarify or consider further revisions to key definitions within the COPPA Rule to avoid inhibiting the development of appropriate and compelling family-friendly websites and online services.

Disney looks forward to continuing to engage with the Commission on these important issues.

Respectfully Submitted,

/s/ Susan Fox
Susan L. Fox
Vice President, Government Relations
THE WALT DISNEY COMPANY
425 3rd Street, SW, Suite 400
Washington, DC 20024

Counsel:
Dana Rosenfeld
Jodie Bernstein
Alysa Hutnik
Matthew Sullivan
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
(202) 342-8400

cc: Mamie Kresses, Esq., Federal Trade Commission
Phyllis Marcus, Esq., Federal Trade Commission

FEDERAL TRADE COMMISSION**16 CFR Part 312**

RIN 3084-AB20

Children's Online Privacy Protection Rule**AGENCY:** Federal Trade Commission ("FTC" or "Commission").**ACTION:** Proposed rule; request for comment.

SUMMARY: The Commission proposes to amend the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), consistent with the requirements of the Children's Online Privacy Protection Act to respond to changes in online technology, including in the mobile marketplace, and, where appropriate, to streamline the Rule. After extensive consideration of public input, the Commission proposes to modify certain of the Rule's definitions, and to update the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions. In addition, the Commission proposes adding a new provision addressing data retention and deletion.

DATES: Written comments must be received on or before November 28, 2011.

ADDRESSES: Interested parties may file a comment online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503" on your comment, and file your comment online at <https://ftcpublic.commentworks.com/ftc/2011coppauleview>, by following the instructions on the Web-based form. If you prefer to file your comment on paper, write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503" on your comment, and mail or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Room H-113 (Annex E), 600 Pennsylvania Avenue, NW., Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Phyllis H. Marcus or Mamie Kresses, Attorneys, Division of Advertising Practices, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580, (202) 326-2854, or (202) 326-2070.

SUPPLEMENTARY INFORMATION:**I. Background**

The COPPA Rule, 16 CFR part 312, issued pursuant to the Children's Online Privacy Protection Act ("COPPA" or "COPPA statute"), 15 U.S.C. 6501 *et seq.*, became effective on April 21, 2000. The Rule imposes certain requirements on operators of Web sites or online services directed to children under 13 years of age, and on operators of other Web sites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (collectively, "operators"). Among other things, the Rule requires that operators provide notice to parents and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13 years of age.¹ The Rule also requires operators to keep secure the information they collect from children and prohibits them from conditioning children's participation in activities on the collection of more personal information than is reasonably necessary to participate in such activities.² The Rule contains a "safe harbor" provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines that would implement the Rule's protections.³

The Commission initiated a review of the Rule on April 21, 2005, pursuant to Section 6507 of the COPPA statute, which required the Commission to conduct a review within five years of the Rule's effective date.⁴ After considering extensive public comment, the Commission determined in March 2006 to retain the Rule without change.⁵

The Commission remains deeply committed to helping to create a safer, more secure online experience for children and takes seriously the challenge to ensure that COPPA continues to meet its originally stated goals, even as online technologies, and children's uses of such technologies, evolve. In light of the rapid-fire pace of technological change since the Commission's 2005 review, including an explosion in children's use of mobile devices, the proliferation of online social networking and interactive gaming, the Commission initiated

review of the COPPA Rule in April 2010 on an accelerated schedule.⁶

On April 5, 2010, the Commission published a document in the **Federal Register** seeking public comment on whether technological changes to the online environment over the preceding five years warranted any changes to the Rule.⁷ The Commission's request for public comment examined each aspect of the COPPA Rule, posing 28 questions for the public's consideration.⁸ The Commission identified several areas where public comment would be especially useful, including examination of whether: The Rule's existing definitions are sufficiently clear and comprehensive, or warrant modification or expansion, consistent with the COPPA statute; additional technological methods to obtain verifiable parental consent should be added to the COPPA Rule, and whether any of the consent methods currently included should be removed; whether the Rule provisions on protecting the confidentiality and security of personal information are sufficiently clear and comprehensive; and the Rule's criteria and process for Commission approval and oversight of safe harbor programs should be modified in any way. The comment period closed on July 12, 2010. During the comment period, on June 2, 2010, the Commission held a public roundtable to discuss in detail several of the areas where public comment was sought, including the application of COPPA's definitions of "Internet," "website," and "online service" to new devices and technologies, the COPPA statute's actual knowledge standard for general audience Web sites and online services, the definition of "personal information," emerging parental consent mechanisms, and COPPA's exceptions to prior parental consent.⁹

In addition to the dialogue at the public roundtable, the Commission received 70 comments from industry representatives, advocacy groups, academics, technologists, and individual members of the public in response to the April 5, 2010 request for public comment.¹⁰ The comments

⁶ The Commission generally reviews each of its trade regulation rules approximately every ten years. Under this schedule, the next COPPA Rule review was originally set for 2017.

⁷ See Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule ("2010 Rule Review"), 75 FR 17089 (Apr. 5, 2010).

⁸ *Id.*

⁹ Information about the June 2, 2010 COPPA Roundtable is located at <http://www.ftc.gov/bcp/workshops/coppa/index.shtml>.

¹⁰ Public comments in response to the Commission's April 5, 2010 **Federal Register**

¹ See Children's Online Privacy Protection Rule, 16 CFR 312.3.

² See 16 CFR 312.7 and 312.8.

³ See 16 CFR 312.10; Children's Online Privacy Protection Rule, 64 FR 59888, 59906, 59908, 59915 (Nov. 3, 1999), available at <http://www.ftc.gov/os/1999/10/64Fr59888.pdf>.

⁴ See 15 U.S.C. 6507; 16 CFR 312.11.

⁵ See Children's Online Privacy Protection Rule, 71 FR 13247 (Mar. 15, 2006) (retention of rule without modification).

addressed the efficacy of the Rule generally, and several possible areas for change.

II. COPPA's Definition of "Child"

The COPPA statute, and by extension, the COPPA Rule, defines as a child "an individual under the age of 13."¹¹ A few commenters suggested that COPPA's protections be broadened to cover a range of adolescents over age 12 and urged the Commission to seek a statutory change from Congress.¹² By contrast, the majority of commenters who addressed this issue expressed concern that expanding COPPA's coverage to teenagers would raise a number of constitutional, privacy, and practical issues.¹³

Recognizing the difficulties of extending COPPA to children ages 13 or older, at least one commenter, the Institute for Public Representation, proposed the need for alternative privacy protections for teenagers. This commenter, while not proposing a statutory change to the definition of "child," called on the Commission to develop a set of privacy protections for teens, consistent with the Fair Information Practices Principles created by the Organization for Economic Cooperation and Development, that would require understandable notices, limited information collection, an opt-in consent process, and access and control rights to data collected from them.¹⁴

In the course of drafting COPPA, Congress looked closely at whether adolescents should be covered by the law. Congress initially considered a requirement that operators make

document are located at <http://www.ftc.gov/os/comments/copparulerev2010/index.shtml>. Comments have been numbered based upon alphabetical order. Comments are cited herein identified by commenter name, comment number, and, where applicable, page number.

¹¹ See 15 U.S.C. 6502(1).

¹² See Andrew Bergen (comment 4); Common Sense Media (comment 12).

¹³ See Sharon Anderson (comment 2); Kevin Brook (comment 6); Center for Democracy and Technology ("CDT") (comment 8), at 5; CTIA (comment 14), at 10; Facebook (comment 22), at 2; Elatia Grimshaw (comment 26); Interactive Advertising Bureau ("IAB") (comment 34), at 6–7; Harold Levy (comment 37); Motion Picture Association of America ("MPAA") (comment 42), at 4; National Cable & Television Association (comment 44), at 5 n.16; NetChoice (comment 45), at 2; Promotion Marketing Association ("PMA") (comment 51), at 5; Berin Szoka (comment 59), at 6; Toy Industry Association of America (comment 63), at 5. Five commenters urged the Commission to consider lowering or eliminating COPPA's age to permit younger children access to a variety of educational online offerings. See Eric MacDonald (comment 38); Mark Moran (comment 41); Steingreaber (comment 58); Karla Talbot (comment 60); Daniel Widrew (comment 67).

¹⁴ See Institute for Public Representation (comment 33), at 42.

reasonable efforts to provide parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17.¹⁵ Ultimately, however, Congress decided to define a "child" as an individual under age 13.¹⁶ The Commission supported this assessment at the time, based in part on the view that young children under age 13 do not possess the level of knowledge or judgment to make appropriate determinations about when and if to divulge personal information over the Internet.¹⁷ The Commission continues to believe that the statutory definition of a child remains appropriate.¹⁸

Although teens face particular privacy challenges online,¹⁹ COPPA's parental notice and consent approach is not designed to address such issues. COPPA's parental notice and consent model works fairly well for young children, but the Commission continues

¹⁵ See *Children's Online Privacy Protection Act of 1998*, S. 2326, 105th Cong. § 3(a)(2)(iii) (1998).

¹⁶ See 15 U.S.C. 6502.

¹⁷ See *Protection of Children's Privacy on the World Wide Web: Hearing on S. 2326 Before the Subcomm. on Communications of the S. Comm. on Commerce, Science & Transportation*, 105th Cong. (1998), at 5 (Statement of Robert Pitofsky, Chairman, Federal Trade Commission), available at <http://www.ftc.gov/os/1998/09/priv98.htm> ("Children are not fully capable of understanding the consequences of divulging personal information online.").

¹⁸ See *Protecting Youths in an Online World: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science & Transportation*, 111th Cong. 14–15 (2010) (Statement of Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission), available at <http://www.ftc.gov/os/testimony/100715toopatestimony.pdf>.

¹⁹ For example, research shows that teens tend to be more impulsive than adults and that they may not think as clearly as adults about the consequences of what they do. See, e.g., Transcript of Exploring Privacy, A Roundtable Series (Mar. 17, 2010), Panel 3: Addressing Sensitive Information, available at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/031710_sess3.pdf; Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (April 14, 2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. As a result, they may voluntarily disclose more information online than they should. On social networking sites, young people may share personal details that leave them vulnerable to identity theft. See Javelin Strategy and Research, 2010 *Identity Fraud Survey Report* (Feb. 2010), available at https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf. They may also share details that could adversely affect their potential employment or college admissions. See, e.g., Commonsense Media, *Is Social Networking Changing Childhood? A National Poll* (Aug. 10, 2009), available at <http://www.commonsemmedia.org/teen-social-media> (indicating that 28 percent of teens have shared personal information online that they would not normally share publicly).

to believe that it would be less effective or appropriate for adolescents.²⁰ COPPA relies on children providing operators with parental contact information at the outset to initiate the consent process. The COPPA model would be difficult to implement for teenagers, as many would be less likely than young children to provide their parents' contact information, and more likely to falsify this information or lie about their ages in order to participate in online activities. In addition, courts have recognized that as children age, they have an increased constitutional right to access information and express themselves publicly.²¹ Finally, given that adolescents are more likely than young children to spend a greater proportion of their time on Web sites and online services that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.²² For all of these reasons, the Commission declines to advocate for a change to the statutory definition of "child."

Although the Commission does not recommend that Congress expand COPPA to cover teenagers, the Commission believes that it is essential that teens, like adults, be provided with clear information about uses of their data and be given meaningful choices about such uses. Therefore, the Commission is exploring new privacy approaches that will ensure that teens—and adults—benefit from stronger privacy protections than are currently generally available.²³

²⁰ *Id.*

²¹ See, e.g., *American Amusement Mach. Ass'n v. Kendrick*, 244 F.3d 572 (7th Cir. 2001) (citing *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–14 (1975)); *Tinker v. Des Moines Indep. Sch. Dist.*, 393 U.S. 503, 511–14 (1969).

²² See *ACLU v. Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008) (citing *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007)) ("Requiring users to go through an age verification process would lead to a distinct loss of personal privacy."); see also *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983) (citing *Butler v. Michigan*, 352 U.S. 380, 383 (1957)) ("The Government may not reduce the adult population * * * to reading only what is fit for children."). See also Berin Szoka (comment 59), at 6.

²³ See *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 36–36 (Dec. 1, 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>; *Protecting Youths in an Online World*, supra note 18, at 14–15 ("The FTC believes that its upcoming privacy recommendations based on its roundtable discussions will greatly benefit teens. The Commission expects that the privacy proposals emerging from this initiative will provide teens both a greater understanding of how their data is used and a greater ability to control such data.").

III. COPPA's "Actual Knowledge" Standard

The COPPA statute applies to two types of operators: (1) Those who operate Web sites or online services directed to children and collect personal information, and (2) those who have *actual knowledge* that they are collecting personal information from a child under age 13.²⁴ The second prong, commonly known as "the actual knowledge standard," holds operators of Web sites directed to teenagers, adults, or to a general audience, liable for providing COPPA's protections *only* when they know they are collecting personal information from a COPPA-covered child (*i.e.*, one under age 13). COPPA therefore was never intended to apply to the entire Internet, but rather to a subset of Web sites and online services.²⁵

Congress did not define the term "actual knowledge" in the COPPA statute, nor did the Commission define the term in the Rule. The case law makes clear that actual knowledge does not equate to "knowledge fairly implied by the circumstances"; nor is actual knowledge "constructive knowledge," as that term is interpreted and applied legally.²⁶ Therefore, the Commission

has advised that operators of general audience Web sites are not required to investigate the ages of their users.²⁷ By contrast, however, operators that ask for—or otherwise collect—information establishing that a user is under the age of 13 trigger COPPA's verifiable parental consent and all other requirements.²⁸

In general, commenters to the Rule review expressed widespread support for Congress's retention of the statutory actual knowledge standard. Supporters find that the standard provides necessary certainty regarding the boundaries of operators' legal liability for COPPA violations.²⁹ Commenters generally felt strongly that a lesser standard, *e.g.*, constructive or implied knowledge, would cause extreme uncertainty for operators of general audience Web sites or online services seeking to comply with the law since they would be obliged either to make guesses about the presence of underage children or to deny access to a wide swath of participants, not only young children.³⁰ According to commenters, such actions would result in greater data collection from all users, including children, in order to determine who should receive COPPA protections (or, alternatively, be denied access to a site). Commenters viewed this result as

contradictory to COPPA's goal of minimizing data collection.³¹

A handful of commenters argued for a different standard. One commenter urged the Commission to require commercial Web site operators to make reasonable efforts to determine if a child is registering online, taking into consideration available technology.³² According to this commenter, Web site operators otherwise face minimal legal risk and business incentive to proactively institute privacy protections for children online. Other commenters, such as the Institute for Public Representation and Microsoft, urged the Commission to adopt clearer guidance on when an operator will be considered to have obtained actual knowledge that it has collected personal information from a child.³³

Despite the limitations of the actual knowledge standard, the Commission is persuaded that this remains the correct standard to be applied to operators of Web sites and online services that are not directed to children. Accordingly, the Commission does not advocate that Congress amend the COPPA statute's actual knowledge requirement at this time. Actual knowledge is far more workable, and provides greater certainty, than other legal standards that might be applied to the universe of general audience Web sites and online services. This is because the actual knowledge standard is triggered only at the point at which an operator becomes aware of a child's age. By contrast, imposing a lesser "reasonable efforts" or "constructive knowledge" standard might require operators to ferret through a host of circumstantial information to determine who may or may not be a child.

As described in detail below, with this Notice of Proposed Rulemaking, the Commission is proposing several modifications to the Rule's definition of "personal information."³⁴ Were the

²⁴ See 15 U.S.C. 6503(a)(1).

²⁵ See MPAA (comment 42), at 10 ("Congress deliberately selected the actual knowledge standard because it served the objective of protecting young children without constraining appropriate data collection and use by operators of general audience Web sites. This standard was selected to serve the goals of COPPA without imposing excessive burdens—including burdens that could easily constrain innovation—on general audience sites and online services").

²⁶ The original scope of COPPA, as indicated in S. 2326 and H.R. 4667, would have applied to any commercial Web site or online service used by an operator to "knowingly" collect information from children. See *Children's Online Privacy Protection Act of 1998*, S. 2326, 105th Cong. § 2(11)(A)(iii) (1998); *Electronic Privacy Bill of Rights Act of 1998*, H.R. 4667, 105th Cong. § 105(7)(A)(iii) (1998). Under federal case law, the term "knowingly" encompasses actual, implied, and constructive knowledge. See *Schmitt v. FMA Alliance*, 398 F.3d 995, 997 (8th Cir. 2005); *Freeman United Coal Mining Co. v. Federal Mine Safety and Health Review Comm'n*, 108 F.3d 358, 363 (D.C. Cir. 1997).

Upon the consideration of testimony from various witnesses, Congress modified the knowledge standard in the final legislation to require "actual knowledge." See *Internet Privacy Hearing: Hearing on S. 2326 Before the Subcomm. on Communications of the S. Comm. on Commerce, Science, and Transportation*, 105th Cong. 1069 (1998). Actual knowledge is generally understood from case law to establish a far stricter standard than constructive knowledge or knowledge implied from the ambient facts. See *United States v. DiSanto*, 86 F.3d 1238, 1257 (1st Cir. 1996) (citing *United States v. Spinney*, 65 F.3d 231, 236 (1st Cir. 1995), for the proposition that "when considering the question of 'knowledge' [it is helpful] to recall that 'the length of the hypothetical knowledge continuum' is marked by 'constructive knowledge' at one end and 'actual knowledge' at

the other with various "gradations," such as "notice of likelihood" in the "poorly charted area that stretches between the poles").

²⁷ See *Children's Online Privacy Protection Rule, Statement of Basis and Purpose* ("1999 Statement of Basis and Purpose"), 64 FR 59888, 59889 (Nov. 3, 1999), available at <http://www.ftc.gov/os/1999/10/64Fr59888.pdf>.

²⁸ See *id.* at 59892 ("Actual knowledge will be present, for example, where an operator learns of a child's age or grade from the child's registration at the site or from a concerned parent who has learned that his child is participating at the site. In addition, although the COPPA does not require operators of general audience sites to investigate the ages of their site's visitors, the Commission notes that it will examine closely sites that do not directly ask age or grade, but instead ask 'age identifying' questions, such as 'what type of school do you go to: (a) elementary; (b) middle; (c) high school; (d) college.' Through such questions, operators may acquire actual knowledge that they are dealing with children under 13").

²⁹ See CTIA (comment 14), at 2; Direct Marketing Association ("DMA") (comment 17), at 8; MPAA (comment 42), at 9; Toy Industry Association, Inc. (comment 63), at 5; Jeffrey Greenbaum, Partner, Frankfurt Kurnit Klein & Selz PC, and J. Beckwith ("Becky") Burr, Partner, WilmerHale, Remarks from *The "Actual Knowledge" Standard in Today's Online Environment* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 78–79 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

³⁰ See Sharon Anderson (comment 2); Boku (comment 5); CDT (comment 9), at 6; CTIA (comment 14), at 2; DMA (comment 17), at 8; Facebook (comment 22), at 7; IAB (comment 34), at 6.

³¹ See CTIA (comment 14), at 2; DMA (comment 17), at 8; Facebook (comment 22), at 7–8.

³² See Harry A. Valetk (comment 66), at 4.

³³ See Institute for Public Representation (comment 33), at 34 (urging the Commission to make clear that an operator can gain actual knowledge where it obtains age information from a source other than the child and where it creates a category for behavioral advertising to children under age 13. "Simply, if an operator decides on, or uses, or purports to know the fact that someone is a child, then that operator has actual knowledge that it is dealing with a child."); Microsoft (comment 39), at 8 (asking the Commission to provide clear guidance on how operators can better meet COPPA's objectives of providing access to rich media content while not undermining parental involvement).

³⁴ For example, the Commission proposes defining as personal information persistent identifiers and screen or user names where they are

Commission to recommend that Congress change COPPA's actual knowledge standard, the changes the Commission proposes to the Rule's definitions might prove infeasible if applied across the entire Internet. The impact of the proposed changes to the definition of personal information are significantly narrowed by the fact that COPPA only applies to the finite universe of Web sites and online services directed to children and Web sites and online services with actual knowledge.

IV. COPPA's Coverage of Evolving Technologies

The Commission's April 5, 2010 **Federal Register** document sought public input on the implications for COPPA enforcement raised by technologies such as mobile communications, interactive television, interactive gaming, and other evolving media.³⁵ The Commission's June 2, 2010 roundtable featured significant discussion on the breadth of the terms "Internet," "website located on the Internet," and "online service" as they relate to the statute and the Rule.

Commenters and roundtable participants expressed a consensus that both the COPPA statute and Rule are written broadly enough to encompass many new technologies without the need for new statutory language.³⁶ First, there is widespread agreement that the statute's definition of "Internet," covering the "myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol," is device neutral.³⁷

used for functions other than or in addition to support for the internal operations of a Web site or online service. The Commission also proposes including identifiers that link the activities of a child across different Web sites or online services, as well as digital files containing a child's image or voice, in the definition. See *infra* Part V.A.(4).

³⁵ See 2010 Rule Review, *supra* note 7, at 17090.

³⁶ See CDT (comment 8), at 2; Edward Felten, Dir. and Professor of Computer Sci. and Pub. Affairs, Princeton Univ. (currently Chief Technologist at the Federal Trade Commission), Remarks from *The Application of COPPA's Definitions of "Internet," "Website," and "Online Service" to New Devices and Technologies* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 13–14 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf ("[T]his was and still is a spot-on definition of what "Internet" means—worldwide interconnection and the use of TCP or IP or any of that suite of protocols.").

³⁷ See CDT (comment 8), at 2. However, two commenters urged the Commission to consider modifying or expanding the definition of "Internet" so as to expressly acknowledge the convergence of technologies, e.g., mobile devices and other

While neither the COPPA statute nor the Rule defines a "Web site located on the Internet," the term is broadly understood to cover content that users can access through a browser on an ordinary computer or mobile device.³⁸ Likewise, the term "online service" broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network.³⁹ The Commission agrees with commenters that a host of current technologies that access the Internet or a wide area network are "online services" currently covered by COPPA and the Rule. This includes mobile applications that allow children to play network-connected games, engage in social networking activities, purchase goods or services online, receive behaviorally targeted advertisements, or interact with other content or services.⁴⁰ Likewise, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location based services, also are online services covered by COPPA and the Rule. The Commission does not believe that the term "online service" needs to be further defined either in the statute or in the Rule.⁴¹

applications that are platform neutral or capable of storing and transmitting data in the manner of a personal computer. See Electronic Privacy Information Center ("EPIC") (comment 19), at 7–8; Jayne Hitchcock (comment 29).

³⁸ See AT&T (comment 3), at 5; Spratt (comment 57); Edward Felten, *supra* note 36, at 15.

³⁹ See John B. Morris, Jr., General Counsel and Director, Internet Standards, Technology and Policy Project, CDT, and Angela Campbell, Institute for Public Representation, Georgetown Univ. Law Ctr., Remarks from *The Application of COPPA's Definitions of "Internet," "Web site," and "Online Service" to New Devices and Technologies* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 16–17 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf. One commenter mentioned that the terms "Internet" and "online" were seemingly intended by Congress to be used interchangeably to mean "the interconnected world-wide network of networks." See Entertainment Software Association (comment 20), at 15 (citing the legislative history, 144 Cong. Rec. S8482–83, Statement of Sen. Bryan (1998)). But see Edward Felten, *supra* note 36, at 19.

⁴⁰ See, e.g., Angela Campbell, *supra* note 39, at 30–31.

⁴¹ The FTC has brought a number of cases alleging violations of COPPA in connection with the operation of an online service, including: *United States v. W3 Innovations LLC*, No. CV–11–03958 (N.D. Cal., filed Aug. 12, 2011) (child-directed mobile applications); *United States v. Playdom, Inc.*, No. SA CV–11–00724 (C.D. Cal., filed May 11, 2011) (online virtual worlds); *United States v. Sony BMG Music Entertainment*, No. 08 Civ. 10730 (S.D.N.Y., filed Dec. 10, 2008) (social networking service); *United States v. Industrious Kid, Inc.*, No. CV–08–0639 (N.D. Cal., filed Jan. 28, 2008) (social networking service); *United States v. Xanga.com, Inc.*, No. 06–CIV–6853 (S.D.N.Y., filed Sept. 7, 2006) (social networking service); and *United States v. Bonzi Software, Inc.*, No. CV–04–1048 (C.D. Cal., filed Feb. 14, 2004) (desktop software application).

Although many mobile activities are online services, it is less clear whether all short message services ("SMS") and multimedia messaging services ("MMS") are covered by COPPA.⁴² One commenter maintained that SMS and MMS text messages cross wireless service providers' networks and short message service centers, not the public Internet, and therefore that such services are not Internet-based and are not "online services."⁴³ However, another panelist at the Commission's June 2, 2010 roundtable cautioned that not all texting programs are exempt from COPPA's coverage.⁴⁴ For instance, mobile applications that enable users to send text messages from their web-enabled devices without routing through a carrier-issued phone number constitute online services.⁴⁵ Likewise, retailers' premium texting and coupon texting programs that register users online and send text messages from the Internet to users' mobile phone numbers are online services.⁴⁶

The Commission will continue to assess emerging technologies to determine whether or not they constitute "Web sites located on the Internet" or "online services" subject to COPPA's coverage.

V. Proposed Modifications to the Rule

As discussed above, commenters expressed a consensus that, given its flexibility and coverage, the COPPA Rule continues to be useful in helping

⁴² See 2010 Rule Review, *supra* note 7, at 17090 (Question 11); see also Denise Tayloe, President, Privo, Inc., Remarks from *Emerging Parental Verification Access and Methods* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 27 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf (questioning whether a "text to vote" marketing campaign is covered by COPPA).

⁴³ See CTIA (comment 14), at 2–5 (citing the Federal Communications Commission's rules and regulations implementing the CAN–SPAM Act of 2003 and the Telephone Consumer Protection Act of 1991, finding that phone-to-phone SMS is not captured by Section 14 of CAN–SPAM because such messages do not have references to Internet domains). The Commission agrees that where mobile services do not traverse the Internet or a wide-area network, COPPA will not apply. See Michael Altschul, Senior Vice President and Gen. Counsel, CTIA, Remarks from *The Application of COPPA's Definitions of "Internet," "Web site," and "Online Service" to New Devices and Technologies* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 19–21 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

⁴⁴ See Edward Felten, *supra* note 36, at 27–28.

⁴⁵ For example, online texting services offered by TextFree, Textie, and textPlus+ that permit users to communicate via text message over the Internet.

⁴⁶ For example, text alert coupon and notification services offered by retailers such as Target and JC Penney.

to protect children as they engage in a wide variety of online activities. The Commission's experience in enforcing the Rule, and public input received through the Rule review process, however, demonstrate the need to update certain Rule provisions. After extensive consideration, the Commission proposes modifications to the Rule in the following five areas: Definitions, Notice, Parental Consent, Confidentiality and Security of Children's Personal Information, and Safe Harbor Programs. In addition to modifying these provisions, the Commission proposes adding a new Rule section addressing data retention and deletion. Each of these changes is discussed in detail below.

A. Definitions (16 CFR 312.2)

The Commission proposes to modify particular definitions to update the Rule's coverage and, in certain cases, to streamline the Rule's language. The Commission proposes modifications to the definitions of "collects or collection," "online contact information," "personal information," "support for the internal operations of the Web site or online service," and "Web site or online service directed to children." The Commission also proposes a minor structural change to the Rule's definition of "disclosure."

(1) Collects or Collection

Section 312.2 of the Rule defines "collects or collection" as:

[T]he gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting that children submit personal information online;

(b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or

(c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.

The Commission proposes amending paragraph (a) to change the term "requesting that children submit personal information online" to "requesting, prompting, or encouraging a child to submit personal information online" in order to clarify that the Rule covers the online collection of personal information both when an operator mandatorily requires it, and when an operator merely prompts or encourages a child to provide such information.

Section 312.2(b) currently defines "collects or collection" to include enabling children to publicly post

personal information (e.g., on social networking sites or on blogs), "except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records."⁴⁷ This aspect of COPPA's definition of "collects or collection" has come to be known as the "100% deletion standard."⁴⁸ Several commenters indicated that this standard, while well-meaning, serves as an impediment to operators' implementation of sophisticated filtering technologies that might aid in the detection and removal of personal information.⁴⁹ Some commenters urged the Commission to revise the Rule to specify the particular types of filtering mechanisms—for example, white lists, black lists, or algorithmic systems—that the Commission believes conform to the Rule's current 100% deletion requirement.⁵⁰ One commenter urged the Commission to exercise caution in modifying the Rule to permit the use of automated filtering systems to strip personal information from posts prior to posting; this commenter urged the Commission to make clear that the use of an automated system *would not* provide an operator with a safe harbor from enforcement action in the case of an inadvertent disclosure of personal information.⁵¹

The Commission has undertaken this Rule review with an eye towards

⁴⁷ Operators who offer services such as social networking, chat, bulletin boards and who do not pre-strip (i.e., completely delete) such information are deemed to have "disclosed" personal information under COPPA's definition of "disclosure." See 16 CFR 312.2.

⁴⁸ See Phyllis Marcus, Remarks from COPPA's Exceptions to Parental Consent Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 310 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

⁴⁹ See Entertainment Software Association (comment 20), at 13–14; Rebecca Newton (comment 46), at 4; see also WiredSafety.org (comment 68), at 15.

⁵⁰ See Berin Szoka (comment 59), Szoka Responses to Questions for the Record, at 19 ("[T]he FTC could * * * allow operators, at least in some circumstances, to use "an automated system of review and/or posting" to satisfy the existing "deletion exception to the definition of collection." In other words, sites could potentially allow children to communicate with each other through chat rooms, message boards, and other social networking tools *without* having to obtain verifiable parental consent if they had in place algorithmic filters that would automatically detect personal information such as a string of seven or ten digits that seems to correspond to a phone number, a string of eight digits that might correspond to a Social Security number, a street address, a name, or even a personal photo—and prevent children from sharing that information in ways that make the information "publicly available"); see also Privo (comment 50), at 5.

⁵¹ See EPIC (comment 19), at 6–7.

encouraging the continuing growth of engaging, diverse, and appropriate online content for children that includes strong privacy protections by design. Children increasingly seek interactive online environments where they can express themselves, and operators should be encouraged to develop innovative technologies to attract children to age-appropriate online communities while preventing them from divulging their personal information. Unfortunately, Web sites that provide children with only limited communications options often fail to capture their imaginations for very long. After careful consideration, the Commission believes that the 100% deletion standard has set an unrealistic hurdle to operators' development and implementation of automated filtering systems.⁵² In its place, the Commission proposes a "reasonable measures" standard whereby operators who employ technologies reasonably designed to capture *all or virtually all* personal information inputted by children should not be deemed to have "collected" personal information. This proposed change is intended to encourage the development of systems, either automated, manual, or a combination thereof, to detect and delete all or virtually all personal information that may be submitted by children prior to its public posting.⁵³

Finally, the Commission proposes simplifying paragraph (c) of the Rule's definition of "collects or collection" to clarify that it includes all means of passive tracking of a child online, irrespective of the technology used. The proposed paragraph removes the language "or use of any identifying code linked to an individual, such as a cookie" and simply states "passive tracking of a child online."

Therefore, the Commission proposes to amend the definition of "collects or collection" so that it reads:

⁵² In fact, inquiries about automated filtering systems, and whether they could ever meet the Commission's current 100% deletion standard, are among the most frequent calls to the Commission's COPPA hotline.

⁵³ In the Commission's experience, establishing a broad standard of reasonableness permits industry to innovate specific security methods that best suit particular needs, and the Commission has set similar "reasonableness" standards in other enforcement arenas. For example, in its law enforcement actions involving breaches of data security, the Commission consistently has required respondents to establish and maintain comprehensive information security programs that are "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." See, e.g., *Ceridian Corp.*, FTC Dkt. No. C-4325 (June 15, 2011); *Lookout Servs., Inc.*, FTC Dkt. No. C-4326 (June 15, 2011).

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

- (a) Requesting, prompting, or encouraging a child to submit personal information online;
- (b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or,
- (c) The passive tracking of a child online.⁵⁴

(2) Disclosure

Section 312.2 of the Rule defines "disclosure" as:

(a) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service and who does not disclose or use that information for any other purpose. For purposes of this definition:

- (1) Release of personal information means the sharing, selling, renting, or any other means of providing personal information to any third party, and
- (2) Support for the internal operations of the Web site or online service means those activities necessary to maintain the technical functioning of the Web site or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(2) and (3); or, (b) Making personal information collected from a child by an operator publicly available in identifiable form, by any means, including by a public posting through the Internet, or through a personal home page posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

The Commission proposes making several minor modifications to this definition that are consistent with the statutory definition. First, the Commission proposes broadening the title of this definition from "disclosure" to "disclose or disclosure" to clarify that in every instance in which the Rule refers to instances where an operator "disclose[s]" information, the definition

of disclosure shall apply. In addition, the Commission proposes moving the definitions of "release of personal information" and "support for the internal operations of the Web site or online service" contained within the definition of "disclosure" to stand-alone definitions within ' 312.2 of the Rule.⁵⁵ This change will clarify what is intended by the terms "release of personal information" and "support for the internal operations of the Web site or online service" where those terms are referenced elsewhere in the Rule and where they are not directly connected with the terms "disclose" or "disclosure."⁵⁶

Therefore, the Commission proposes to amend the definition of "disclosure" to read:

Disclose or disclosure means, with respect to personal information:

- (a) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and,
 - (b) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.
- (3) "Release of personal information"

The Commission proposes to define the term "release of personal information" separately from its current inclusion within the definition of "disclosure." Since the term applies to provisions of the Rule that do not relate solely to disclosures,⁵⁷ this stand-alone definition will provide greater clarity as to the terms' applicability throughout the Rule. In addition, the Commission proposes technical changes to clarify that the term "release of personal information" primarily addresses business-to-business uses of personal information. Public disclosure of personal information is covered by paragraph (b) of the definition of

"disclosure." Therefore, the Commission proposes to revise the definition of "release of personal information" so that it reads:

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

- (4) "Support for the internal operations of the Web site or online service"

The Commission also proposes separating out the term "support for the internal operations of the Web site or online service" from the definition of "disclosure." The Commission recognizes that the term "support for internal operations of the Web site or online service"—*i.e.*, activities necessary to maintain the technical functioning of the Web site or online service—is an important limiting concept that warrants further explanation. The Rule recognizes that information that is collected by operators for the sole purpose of support for internal operations should be treated differently than information that is used for broader purposes.

The term currently is a part of the definitions of "disclosure" and "third party" within the Rule. As explained below, the Commission proposes to expand the definition of "personal information" to include "screen or user names" and "persistent identifiers," when such items are used for functions other than or in addition to "support for the internal operations of the Web site or online service."⁵⁸ In proposing to create a separate definition of "support for the internal operations of a Web site or online service," the Commission also proposes to expand that definition to include "activities necessary to protect the security or integrity of the Web site or online service." With this change, the Commission recognizes operators' need to protect themselves or their users from security threats, fraud, denial of service attacks, user misbehavior, or other threats to operators' internal operations.⁵⁹ In addition, the Commission proposes adding the limitation that information collected for such purposes may not be used or disclosed for any other purpose, so that if there is a secondary use of the information, it becomes "personal information" under the Rule.

The Commission recognizes that operators use persistent identifiers and screen names to aid the functionality and technical stability of Web sites and online services and to provide a good user experience, and the Commission does not intend to limit operators'

⁵⁴ One commenter, EPIC, expressed the opinion that the Rule's reference to information collected "by any means" in the definition of "collects or collection" is ambiguous with regard to information acquired offline that is uploaded, stored, or distributed to third parties by operators. See EPIC (comment 19), at 5. However, Congress limited the scope of COPPA to information that an operator collects *online* from a child; COPPA does not govern information collected offline. See 15 U.S.C. 6501(8) (defining the personal information as "individually identifiable information about an individual collected online. * * *"); 144 Cong. Rec. S11657 (Oct. 7, 1998) (Statement of Sen. Bryan) ("This is an online children's privacy bill, and its reach is limited to information collected online from a child.").

⁵⁵ The Commission also proposes minor changes to the definition of "support for the internal operations of a Web site or online service," as described in Part V.A(5), below.

⁵⁶ For example, the term "support for the internal operations of the Web site or online service" is included within the proposed revisions to the definition of "personal information." See *infra* Part V.A(5). The term "release of personal information" is included within the proposed revised provision to ' 312.8 regarding "Confidentiality, security, and integrity of personal information collected from children." See *infra* Part V.D.

⁵⁷ See, e.g., discussion regarding 16 CFR 312.8 (confidentiality, security and integrity of children's personal information), *infra* Part V.D.

⁵⁸ See *infra* Part V.(5)(b) and (c).

⁵⁹ See WiredSafety.org (comment 68), at 17.

ability to collect such information from children for those purposes. However, the Commission also recognizes that such identifiers may be used in more expansive ways that affect children's privacy. In the sections that follow, the Commission sets forth the parameters within which operators may collect and use screen names and persistent identifiers without triggering COPPA's application.⁶⁰

The Commission proposes to revise the definition of "support for the internal operations of Web site or online service" so that it states:

Support for the internal operations of the Web site or online service means those activities necessary to maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, or to fulfill a request of a child as permitted by § 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose.

(5) Online Contact Information

Section 312.2 of the Rule defines "online contact information" as "an e-mail address or any other substantially similar identifier that permits direct contact with a person online." The Commission proposes to clarify this definition to flag that the term covers *all* identifiers that permit direct contact with a person online, and to eliminate any inconsistency between the stand-alone definition of online contact information and the use of the same term within the Rule's definition of "personal information."⁶¹ The revised definition set forth below adds commonly used forms of online identifiers, including instant messaging user identifiers, voice over internet protocol (VOIP) identifiers, and video chat user identifiers. The proposed definition makes clear, however, that the identifiers included are not intended to be exhaustive, and may include other substantially similar identifiers that permit direct contact with a person online.

Therefore, the Commission proposes to amend the definition of "online contact information" to state:

⁶⁰ *Id.*

⁶¹ The Rule currently defines as personal information "an e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address." 16 CFR 312.2 (paragraph (c), definition of "personal information"). The Commission also proposes removing the listing of identifiers from the definition of personal information and substituting the simple phrase "online contact information" instead. See *infra* Part V.A.(4)(a). By doing so, the Commission hopes to streamline the Rule's definitions in a way that is useful and accessible for operators.

Online contact information means an e-mail address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

(6) Personal Information

The COPPA statute defines personal information as individually identifiable information about an individual collected online, including:

- (A) A first and last name;
- (B) A home or other physical address including street name and name of a city or town;
- (C) An e-mail address;
- (D) A telephone number;⁶²
- (E) A Social Security number;
- (F) Any other identifier that the

Commission determines permits the physical or online contacting of a specific individual; or
(G) information concerning the child or the parents of that child that the Web site collects online from the child and combines with an identifier described in this paragraph.⁶³

As explained below, the Commission proposes to use this statutorily granted authority in paragraph (F) to modify, and in certain cases, expand, upon the Rule's definition of "personal information" to reflect technological changes.

a. Online Contact Information (Revised Paragraph (c))

The Commission proposes to replace existing paragraph (c) of the Rule's definition of "personal information," which refers to "an e-mail address or other online contact information including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address," with the broader term "online contact information," as newly defined.⁶⁴ Moreover, as discussed immediately below, the Commission

⁶² The term "telephone number" includes landline, web-based, and mobile phone numbers.

⁶³ 15 U.S.C. 6502(8). The Federal Trade Commission originally used the authority granted under Section 6502(8)(F) to define personal information under the COPPA Rule to include the following pieces of information not specifically listed in the statute:

- Other online contact information, including but not limited to an instant messaging user identifier;
- A screen name that reveals an individual's e-mail address;
- A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; and,
- A combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting.

⁶⁴ See *supra* Part V.A.(4)(a).

proposes to move the existing reference to a "screen name" to a separate item within the definition of "personal information."

b. Screen or User Names (Revised Paragraph (d))

Currently, screen names are considered "personal information" under COPPA only when they reveal an individual's e-mail address. The Commission proposes instead that screen (or user) names be categorized as personal information when they are used for functions other than, or in addition to, support for the internal operations of the Web site or online service. This change reflects the reality that screen and user names increasingly have become portable across multiple Web sites or online services, and permit the direct contact of a specific individual online regardless of whether the screen or user names contain an e-mail address.⁶⁵

The proposed definition exempts screen or user names that are used solely to maintain the technical functioning of the Web site or online service. This qualification is intended to retain operators' ability to utilize screen or user names *within* a Web site or online service (absent the collection, use, or disclosure of *other* personal information) without obtaining prior parental consent. Accordingly, an operator may allow children to establish screen names for use within a site or service. Such screen names may be used for access to the site or service, to identify users to each other, and to recall user settings. However, where the screen or user name is used for purposes other than to maintain the technical functioning of the Web site or online service, the screen name becomes "personal information" under the proposed Rule.

c. Persistent Identifiers (Revised Paragraph (g)) and Identifiers Linking a Child's Online Activities (New Paragraph (h))

The existing Rule includes as personal information "a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information."⁶⁶ In its 1999 Statement of Basis and Purpose, the Commission discussed persistent identifiers that automatically are collected by Web sites, such as static IP addresses and

⁶⁵ See, e.g., OpenId, Windows Live ID, and the Facebook Platform.

⁶⁶ See paragraph (f) to the definition of "personal information." 16 CFR 312.2.

processor serial numbers, stating that “unless such identifiers are associated with other individually identifiable personal information, they would not fall within the Rule’s definition of ‘personal information.’” Moreover, with respect to information stored in cookies, the Commission stated that “[i]f the operator either collects individually identifiable information using the cookie or collects non-individually identifiable information using the cookie that is combined with an identifier, then the information constitutes ‘personal information’ under the Rule, regardless of where it is stored.”⁶⁷ Taken together, these statements limit COPPA’s coverage of persistent identifiers solely to those identifiers that are otherwise linked to “personal information” as defined by the Rule.

Developments in technology in the intervening twelve years since the COPPA Rule was issued, and the resulting implications for consumer privacy, have led to a widespread reexamination of the concept of “personal information” and of the types of information COPPA should cover.⁶⁸ While it is clear that COPPA always was intended to regulate an operator’s ability to obtain information from, and market back to, children,⁶⁹ methods of marketing online have burgeoned in recent years. In this regard, the Commission sought comment on whether certain identifiers, such as IP

address, zip code, date of birth, gender, and information collected in connection with online behavioral advertising, should now be included within the Rule’s definition of “personal information.”⁷⁰

Numerous comments to the Rule review addressed this question.⁷¹ Several commenters opposed such an expansion, pointing out that the collection of certain identifiers, such as IP addresses, are integral to the delivery of online content.⁷² According to these commenters, if an IP address, on its own, were to be included within the definition of “personal information,” virtually every Web site or online service directed to children would be subject to COPPA’s requirements, regardless of whether any additional information is collected, used, or disclosed, because a browser’s communication with a Web site typically reveals the user’s IP address to the Web site operator. Commenters especially expressed concern about operators’ ability to obtain prior verifiable parental consent in such situations.⁷³ In addition, some commenters noted that an IP address may not lead an operator to a specific individual, but rather, indicate only a particular computer or computing device shared by a number of individuals.⁷⁴

Several other commenters addressed the question of whether identifiers such as cookies or other technologies used to track online activities should be included within the definition of “personal information.” As with the comments regarding IP addresses, these commenters maintained that uses of cookies and other tracking devices do not result in the contacting of specific individuals online as contemplated by Congress in the COPPA statute.⁷⁵ Moreover, some commenters asserted that these technologies can be used for

a number of beneficial purposes, *e.g.*, some operators use cookies to protect children from inappropriate advertising (and conversely, to deliver only appropriate advertising); other operators use cookies to personalize children’s online experiences. Finally, these commenters contended that expanding COPPA to include cookies and other online behavioral advertising technologies is unnecessary because existing self-regulatory principles for online behavioral advertising are sufficient to curtail targeted advertising to children.⁷⁶

By contrast, several commenters asserted that identifiers such as cookies and IP addresses can be used by online operators to track and communicate with *specific* individuals and should be included within COPPA’s categories of information considered to be personal.⁷⁷

After careful consideration, the Commission believes that persistent identifiers can permit the contacting of a specific individual, and thus, with the limitations described below, should be included as part of a revised definition of “personal information” in the COPPA Rule. The Commission does not agree with commenters who argue that persistent identifiers only allow operators to contact a specific device or computer. Information that “permits the physical or online contacting of a specific individual” does not mean information that permits the contacting of only a single individual, to the exclusion of all other individuals. For example, the COPPA statute includes within the definition of “personal information” a home address alone or a phone number alone—information that is often applicable to an entire household. The Commission believes this reflects the judgment of Congress that an operator who collects this information is reasonably likely to be able to contact a specific individual, even without having collected other identifying information. The Commission believes the same is true of persistent identifiers.

Moreover, increasingly, consumer access to computers is shifting from the model of a single, family-shared,

⁶⁷ See 1999 Statement of Basis and Purpose, 64 FR 59888, 59892–93.

⁶⁸ Commission staff recognized in its 2009 online behavioral advertising report that, “in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data.” FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, 21–22 (Feb. 2009), available at <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>. Similarly, the Federal Trade Commission 2010 Staff Privacy Report cited widespread recognition among industry and academics that the traditional distinction between the two categories of data has eroded, and that information practices and restrictions that rely on this distinction are losing their relevance. See Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 35–36.

⁶⁹ See 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan) (“Unfortunately, the same marvelous advances in computer and telecommunication technology that allow our children to reach out to new resources of knowledge and cultural experiences are also leaving them unwittingly vulnerable to exploitation and harm by deceptive marketers and criminals * * *. Much of this information appears to be harmless, but companies are attempting to build a wealth of information about you and your family without an adult’s approval—a profile that will enable them to target and to entice your children to purchase a range of products. The Internet gives marketers the capability of interacting with your children and developing a relationship without your knowledge”).

⁷⁰ See 2010 Rule Review, *supra* note 7, at 17090.

⁷¹ See, *e.g.*, BOKU (comment 5); CDT (comment 8); DMA (comment 17), at 6–9; Entertainment Software Association (comment 20), at 17–18; Google, Inc. (comment 24), at 6–7; Institute for Public Representation (comment 33), at 21; IAB (comment 34), at 3–5; Interstate Commerce Coalition (comment 35), at 2; Microsoft Corporation (comment 39), at 9–10; MPAA (comment 42), at 6–7; NetChoice (comment 45), at 6–7; Paul Ohm (comment 48); TechAmerica (comment 61), at 5–6; Toy Industry Association, Inc. (comment 63), at 7–10; TRUSTe (comment 64), at 3–5.

⁷² See Google, Inc. (comment 24), at 7; Internet Commerce Coalition (comment 35), at 2–3.

⁷³ See, *e.g.*, Entertainment Software Association (comment 20), at 18; Interstate Commerce Coalition (comment 35), at 2.

⁷⁴ See Toy Industry Association, Inc. (comment 63), at 9; TRUSTe (comment 64), at 5.

⁷⁵ See Facebook (comment 22), at 6; Microsoft Corporation (comment 39), at 9; Toy Industry Association, Inc. (comment 63), at 7.

⁷⁶ See CDT (comment 8, at 8) (referring to the Network Advertising Initiative’s 2008 *NAI Principles Code of Conduct*); Entertainment Software Association (comment 20), at 19 (referring to the *Self-Regulatory Principles for Online Behavioral Advertising* issued by the American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus in July 2009); Facebook (comment 22), at 7.

⁷⁷ See Common Sense Media (comment 12), at 8; EPIC (comment 19), at 9; Institute for Public Representation (comment 33), at 21.

personal computer to the widespread distribution of person-specific, Internet-enabled, handheld devices to each member within a household, including children.⁷⁸ Such handheld devices often have one or more unique identifiers associated with them that can be used to persistently link a user across Web sites and online services, including mobile applications.⁷⁹ With this change in computing use, operators now have a better ability to link a particular individual to a particular computing device.

At the same time, the Commission is mindful of the concerns raised by commenters that including persistent identifiers within the definition of personal information, without further qualification, would hinder operators' ability to provide basic online services to children. Several commenters indicated that Web sites and online services must identify and use IP addresses to deliver content to computers; if IP addresses, without more, were treated as "personal information" under COPPA, a site or service would be liable for collecting personal information as soon as a child landed on its home page or screen.⁸⁰ The Commission agrees that such an approach is over-broad and unworkable.⁸¹

⁷⁸ See Common Sense Media, *Do Smart Phones = Smart Kids? The Impact of the Mobile Explosion on America's Kids, Families, and Schools* (Apr. 2010), available at <http://www.common SenseMedia.org/smartphones-smartkids> (citing a study from the NPD Group, Inc. finding that 20% of U.S. children ages 4–14 owned a cell phone in 2008); N. Jackson, "More Kids Can Work Smartphones Than Can Tie Their Own Shoes," *The Atlantic* (Jan. 24, 2011), available at <http://www.theatlantic.com/technology/archive/2011/01/more-kids-can-work-smartphones-than-can-tie-their-own-shoes/70101/>; see also S. Smith, "Now It's Personal: Mobile Nears the Privacy Third Rail," *Behavioral Insider* (Apr. 22, 2011), available at http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149196 (warning that "[m]any of the arguments used to assuage worries about digital privacy online are simply less effective [in the mobile space]. When data can be tied to specific device IDs, times and location, insistence that the resulting data is 'anonymized' (no matter how true it may be) is very hard for the layman to swallow.").

⁷⁹ Sometimes called "processor serial numbers," "device serial numbers," or "unique device identifier," unique identifiers refer to software-readable or physical numbers embedded by manufacturers into individual processors or devices. See, e.g., J. Valentino-DeVries, *Unique Phone ID Numbers Explained*, *Wall St. J.* (Dec. 19, 2010), available at <http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/>.

⁸⁰ See CDT (comment 9), at 7–8; DMA (comment 17), at 6; Entertainment Software Association (comment 20), 17–18; Google (comment 24), 7; Internet Commerce Coalition (comment 35), at 2–3; and TechAmerica (comment 61), at 6.

⁸¹ As some commenters noted, it would be impracticable to obtain verifiable parental consent prior to the collection of an IP address for purposes

The Commission believes that when a persistent identifier is used only to support the internal operations of a Web site or online service, rather than to compile data on specific computer users, the concerns underlying COPPA's purpose are not present.⁸² Accordingly, the Commission proposes to modify the definition of "personal information" by revising paragraph (g), and adding a paragraph (h), as follows:

(g) A persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the Web site or online service;

(h) an identifier that links the activities of a child across different Web sites or online services;

Proposed paragraph (g)—which covers persistent identifiers *where they are used for functions other than, or in addition to, support for the internal operations of the Web site or online service*—is designed not to interfere with operators' ability to deliver content to children within the ordinary operation of their Web sites or online services. This limitation takes into account the comments expressing concern about the potential for COPPA to interfere with the ordinary operation of Web sites or online services.⁸³ The new language in the definition would permit operators' use of persistent identifiers for purposes such as user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft. However, the new language would require parental notification and consent prior to the collection of persistent identifiers where they are used for purposes such as amassing data on a child's online activities or behaviorally targeting advertising to the child. Therefore, operators such as network advertisers may not claim the collection of persistent identifiers as a technical

of delivering online content, since Web site operators would not know at that point in time that the Web site visitor was a child, and would have no means of obtaining consent from that child's parent. See, e.g., Internet Commerce Coalition (comment 35), at 2.

⁸² See 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan).

⁸³ See Boku (comment 5) (encouraging the Commission to regulate the use of identifiers such as IP address, device data, or any other data automatically captured during interaction with a user and a web site rather than the data capture itself or the storage of such data; see also CDT (comment 8), at 8 (asserting that a prohibition on the mere collection of this data would undermine the very functioning of the Internet).

function under the "support for internal operations" exemption.

New paragraph (h) of the definition of "personal information" is intended to serve as a catch-all category covering the online gathering of information about a child over time for the purposes of either online profiling or delivering behavioral advertising to that child.⁸⁴ For example, an advertising network or analytics service that tracks a child user across a set of Web sites or online services, but stores this information in a separate database rather than with the persistent identifier, would be deemed to have collected personal information from the child under this proposed paragraph.

Several commenters stated that industry self-regulatory efforts more effectively address the treatment of online behavioral advertising to children than would regulation in this area. For example, citing the industry's 2009 *Self-Regulatory Principles for Online Behavioral Advertising*, the Direct Marketing Association asserted that "robust self-regulation is the best and most appropriate way to address privacy concerns in connection with online behavioral advertising, including concerns related to children."⁸⁵

The Commission finds this argument unpersuasive. Although self-regulation can play an important role in consumer protection, Congress specifically directed the Commission to promulgate and implement regulations covering the online collection, use, and disclosure of children's personal information. To the extent that children's personal information is collected in connection with behavioral advertising, such information should be protected under the Rule. While self-regulatory programs can be valuable in promoting compliance, the proposed revision implements the COPPA statute and is enforceable by law.⁸⁶

⁸⁴ "Online behavioral advertising" is the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests. See *Self-Regulatory Principles for Online Behavioral Advertising*, *supra* note 68, at i.

⁸⁵ DMA (comment 17), at 7 (directing the Commission's attention to *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), at 16–17, available at <http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf>). See also Entertainment Software Association (comment 20), at 19; Facebook (comment 22), at 7; IAB (comment 34), at 3; Microsoft (comment 39), at 9–10; Mobile Marketing Association (comment 40), at 3; Toy Industry Association (comment 63), at 9.

⁸⁶ Although it is unclear from the record before the Commission whether operators currently are directing online behavioral advertising to children (various members of industry have informed Commission staff that they do not believe such activity is occurring while media reports have indicated the widespread presence of tracking tools

d. Photographs, Videos, and Audio Files (New Paragraph (i))

The Rule's existing definition of "personal information" includes photographs only when they are combined with "other information such that the combination permits physical or online contacting." Given the prevalence and popularity of posting photos, videos, and audio files online, the Commission has reevaluated the privacy and safety implications of such practices as they pertain to children. Inherently, photos can be very personal in nature. Also, photographs of children, in and of themselves, may contain information, such as embedded geolocation data, that permits physical or online contact.⁸⁷ In addition, facial recognition technology can be used to further identify persons depicted in photos.⁸⁸

The Commission believes that, with respect to the subset of Web sites and online services directed to children or having actual knowledge of collecting personal information from children, broader Rule coverage of photos is

on children's Web sites, see Steven Stecklow, *On the Web, Children Face Intensive Tracking*, Wall St. J., Sept. 17, 2010), the Commission notes that the self-regulatory guidelines cited by the commenters do not expressly require prior parental consent for such advertising to occur. Rather, operators who adhere to such guidelines are merely cautioned that they should comply with COPPA when engaging in online behavioral advertising. See *Self-Regulatory Principles for Online Behavioral Advertising*, supra note 85, at 16–17 ("Entities should not collect 'personal information', as defined in the Children's Online Privacy Protection Act ('COPPA'), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA"). Moreover, the self-regulatory standards cited by commenters do not collectively represent all operators subject to COPPA.

⁸⁷ In addition to the personal information that may be viewable in a photograph or video, geolocation data is commonly embedded as hidden "metadata" within these digital images. These data usually consist of latitude and longitude coordinates, and may also include altitude, bearing, distance, and place names. Such geolocation information may be used by operators and may also be accessed by the viewing public. The Commission proposes to specifically enumerate "geolocation information" as a separate category of "personal information" under the Rule. See *infra* Part V.A.(4)(e).

⁸⁸ See M. Geuss, "Facebook Facial Recognition Could Get Creepy: new facial recognition technology used to identify your friends in photos could have some interesting applications—and some scary possibilities," PC World (Apr. 26, 2011), available at http://www.pcworld.com/article/226228/facebook_facial_recognition_its_quiet_rise_and_dangerous_future.html (discussing Facebook's facial recognition technology, and similar technologies offered by services such as Viewdle, Fotobounce, Picasa, iPhoto, and Face.com).

warranted.⁸⁹ In addition, the Commission believes that the Rule's definition of "personal information" should be expanded to include the posting of video and audio files containing a child's image or voice, which, similarly to photos, may enable the identification and contacting of a child. Therefore, the Commission proposes to create a new paragraph (i) of the definition of "personal information" that states:

(i) A photograph, video, or audio file where such file contains a child's image or voice; This proposed change will ensure that parents are given notice and the opportunity to decide whether the posting of images or audio files is an activity in which they wish their children to engage.

e. Geolocation Information (New Paragraph (j))

In recent years, geolocation services have become ubiquitous features of the personal electronics market.⁹⁰ Numerous commenters raised with the Commission the issue of the potential risks associated with operators' collection of geolocation information from children. Some commenters urged the Commission to expressly modify the Rule to include geolocation information, given the current pervasiveness of such technologies and their popularity among children.⁹¹ Others maintained that geolocation information is already covered by existing paragraph (b) of the Rule's definition of "personal information," which includes "a home or other physical address including

⁸⁹ Although the Commission received little comment on this topic, one individual commenter, as well as the Commission-approved COPPA safe harbor, TRUSTe, strongly supported this approach. See Gregory Schiller (comment 47); Office of the State Attorney—15th Judicial Circuit in and for Palm Beach County, Florida (comment 47); TRUSTe (comment 64), at 4; Maureen Cooney, Chief Privacy Officer, TRUSTe, Remarks from *COPPA's Definition of "Personal Information"* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 191–92 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

⁹⁰ For example, geolocation-based navigation tools help users reach destinations, find local businesses or events, find friends and engage in social networking, "check in" at certain locations, and link their location to other activities. Many users access geolocation services through mobile devices. However, devices such as laptop and desktop computers, tablets, and in-car navigation and assistance systems also may be used to access such services. Geolocation information may be used once for a single purpose, or it may be stored or combined with other information to produce a history of a user's activities or a detailed profile for advertising or other purposes. See ACLU, "Location Based Services: Time For a Privacy Check-In" 1, 3 (Nov. 2010) available at <http://dotrights.org/sites/default/files/lbs-white-paper.pdf>.

⁹¹ See, e.g., EPIC (comment 19), at 8.

street name and name of a city or town"⁹²

Technologies that collect geolocation information can take a variety of forms and can communicate location with varying levels of precision. Generally speaking, most commonly used location tracking technologies are capable of revealing a person's location at least down to the level of a street name and the name of a city or town.⁹³ In the Commission's view, any geolocation information that provides precise enough information to identify the name of a street and city or town is covered already under existing paragraph (b) of the definition of "personal information." However, because geolocation information may be presented in a variety of formats (e.g., coordinates or a map), and in some instances may be more precise than street name and name of city or town, the Commission proposes making geolocation information a stand-alone category within that definition.

Those commenters who opposed the inclusion of geolocation information within COPPA's definition of "personal information" argued that such information cannot be used to identify a specific individual, but only a device.⁹⁴ However, as discussed above, the Commission finds this argument unpersuasive.⁹⁵ Physical address, including street name and name of city or town, alone is considered personal information under COPPA. Accordingly, geolocation data that provides information at least equivalent to "physical address" should be covered as personal information.

f. Date of Birth, Gender, and ZIP Code

Several commenters recommended that the Commission include date of birth, gender, or ZIP code in the definition of "personal information."⁹⁶ The Commission gave careful thought to these recommendations, but is not proposing to include these items within

⁹² See Institute for Public Representation (comment 33), at 26; TRUSTe (comment 64), at 4. See also Jules Polonetsky, Director, Future of Privacy Forum; Paul Ohm, Professor, Univ. of Colorado Law School; Sheila A. Millar, Partner, Keller & Heckman LLP; Matt Galligan, Founder and CEO, SimpleGeo; Heidi C. Salow, Of Counsel, DLA Piper, Remarks from *COPPA's Definition of "Personal Information"* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 195, 205–07 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

⁹³ See ACLU, supra note 90, at 9.

⁹⁴ See DMA (comment 17), at 7–8; MPAA (comment 42), at 6–7; Net Choice (comment 45), at 6.

⁹⁵ See supra Part V.A.(6)(c).

⁹⁶ See EPIC (comment 19), at 8–9; Institute for Public Representation (comment 33), at 33.

the definition because the Commission does not believe that any one of these items of information, alone, permits the physical or online contacting of a specific individual. However, the Commission seeks input as to whether the combination of date of birth, gender, and ZIP code provides sufficient information to permit the contacting of a specific individual such that this combination of information should be included in the Rule as “personal information.”⁹⁷ Moreover, there is a question whether an operator’s collection of “ZIP+4” may, in some cases, be the equivalent of a physical address. “ZIP+4 Code consists of the original 5-digit ZIP Code plus a 4-digit add-on code that identifies a geographic segment within the 5-digit delivery area, such as a city block, office building, individual high-volume receiver of mail, or any other unit that would aid efficient mail sorting and delivery.”⁹⁸ The Commission seeks input on whether ZIP+4 is the equivalent of a physical address and whether it should be added to the Rule.⁹⁹

g. Other Collections of Information

Taking a different view of “personal information,” one commenter argued that the Commission should move away from identifying new particular individual items of personal information, and instead add to the definition “any collection of more than twenty-five distinct categories of information about a user.”¹⁰⁰ This proposed definition is based on the premise that above a certain quantity threshold, the information an operator holds about a particular user becomes sufficiently identifying so as to be “personal.” The Commission recognizes the potential for collections of diverse bits of information to permit the identification of a specific individual; however, the record is not sufficiently developed at this time to support a quantity-based approach to defining personal information. Without greater specificity, a quantity-based approach would not provide operators with sufficient certainty to determine which collections and combinations of information trigger the Rule’s

⁹⁷ See *infra* Part X. at Question 9(b). Commenter Paul Ohm cites to several studies finding that a significant percentage of individuals can be uniquely identified by the combination of these three pieces of information. See Paul Ohm (comment 48), at 3, note 7.

⁹⁸ See United States Postal Service, Frequently Asked Questions, ZIP Code Information, [http://faq.usps.com/eCustomer/iq/usps/search “ZIP Code Information”](http://faq.usps.com/eCustomer/iq/usps/search%20ZIP%20Code%20Information); then follow “ZIP Code Information” hyperlink (last visited September 12, 2011).

⁹⁹ See *infra* Part X. at Question 9(c).

¹⁰⁰ See Paul Ohm (comment 48), at 2.

requirements and which do not. As a result, this standard would be difficult for operators to implement, as well as for the government to enforce.¹⁰¹ The Commission believes that setting bright-line categories of personal information, while potentially both over- and under-inclusive, provides greater certainty for operators seeking to follow the Rule.

(7) Web Site or Online Service Directed to Children

The Commission also considered whether any changes needed to be made to the Rule’s definition of “website or online service directed to children.” The current definition is largely a “totality of the circumstances” test that provides sufficient coverage and clarity to enable Web sites to comply with COPPA, and the Commission and its state partners to enforce COPPA.¹⁰² Few commenters addressed the definition. However, one commenter, the Institute for Public Representation, suggested that the Rule be amended so that a Web site *per se* should be deemed “directed to children” if audience demographics show that 20% or more of its visitors are children under age 13.¹⁰³

The current definition of “website or online service directed to children” already notes that the Commission will consider competent and reliable empirical evidence of audience composition as part of a totality of circumstances analysis. The Commission’s experience with online audience demographic data in both its studies of food marketing to children and marketing violent entertainment to children shows that such data is neither available for all Web sites and online services, nor is it sufficiently reliable, to adopt it as a *per se* legal standard.¹⁰⁴

¹⁰¹ Professor Ohm acknowledges that “most websites probably do not count their data in this way today, so the regulation will require some websites to expend modest new resources to comply. Moreover, every time a website decides to collect new categories of information from users, it needs to recalculate its count.” *Id.* at 8–9.

¹⁰² See, e.g., *United States v. Playdom, Inc.*, No. SA CV–11–00724 (C.D. Cal., filed May 11, 2011) (finding defendants’ Pony Stars Web site to be “directed to children”); *United States v. Industrious Kid, Inc.*, No. CV–08–0639 (N.D. Cal., filed Jan. 28, 2008); *United States v. UMG Recordings, Inc.*, No. CV–04–1050 (C.D. Cal., filed Feb. 17, 2004); *United States v. Bonzi Software, Inc.*, No. CV–04–1048 (C.D. Cal., filed Feb. 17, 2004).

¹⁰³ See Institute for Public Representation (comment 33), at iii (urging the Commission to adopt the same threshold, 20%, used in the Commission’s 2007 food marketing Orders to File a Special Report).

¹⁰⁴ In the context of the Commission’s food marketing studies, food marketers were required to identify and report Web site expenditures targeted to children based on a number of criteria, one of which was whether audience demographic data indicated that 20% or more of visitors to a Web site were children ages 2–11. See Fed. Trade Comm’n,

Accordingly, the Commission declines to adopt a standard akin to the 20% standard proposed by the Institute for Public Representation.

However, the Commission proposes minor modifications to the definition, as follows. First, as part of the totality of the circumstances analysis, the Commission proposes modifying the term “audio content” to include musical content. In addition, the Commission proposes adding the presence of child celebrities, and celebrities who appeal to children, within the non-exclusive set of indicia it will use to determine whether a Web site or online service is directed to children. In the Commission’s experience, both music and the presence of celebrities are strong indicators of a Web site or online service’s appeal to children. Finally, the Commission proposes reordering the language of the definition so that the terms “animated characters” and “child-oriented activities and incentives” are addressed alongside the other indicia of child-directed content.

Therefore, the proposed definition of “Web site or online service directed to children” reads:

Website or online service directed to children means a commercial Web site or online service, or portion thereof, that is targeted to children. Provided, however, that a commercial Web site or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In determining whether a commercial Web site or online service, or a portion thereof, is targeted to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

B. Notice (16 CFR 312.4)

The linchpins of the COPPA Rule are its parental notice and consent requirements. Providing parents with clear and complete notice of operators’ information practices is the necessary first step in obtaining informed consent

Order to File Special Report, B–3, note 14 (July 31, 2007) available at <http://www.ftc.gov/os/06/orders/foodmktg6b/070731boskovichfarmssixb.pdf>. There, the 20% threshold was not used as a basis to impose legal liability for a Rule violation.

from parents. COPPA requires that parents be notified in two ways: on the operator's Web site or online service (the "online notice," which typically takes the form of a privacy policy), and in a notice delivered directly to a parent whose child seeks to register on the site or service (the "direct notice"). The current Rule requires that operators provide extensive information about their children's privacy practices in their online notice. While the Rule states that the direct notice must contain the information an operator includes in its online notice as well as certain additional information, in the past, the Commission has indicated that operators may truncate the information in the direct notice by providing a hyperlink to their online privacy policy.¹⁰⁵

Outside the COPPA context, in recent years, the Commission has begun to urge industry to provide consumers with notice and choice about information practices at the point consumers enter personal data or before accepting a product or service.¹⁰⁶ The analogous point of entry under COPPA would be the direct notice, which has the potential to provide parents with the best opportunity to consider an operator's information practices and to determine whether to permit children's engagement with such operator's Web site or online service. Therefore, the Commission proposes to revise the notice requirements to reinforce COPPA's goal of providing complete and clear information in the direct notice, and to rely less heavily on the online notice or privacy policy as a means of providing parents with information about operators' information practices.¹⁰⁷

(1) Notice on the Web site or Online Service (Revised Paragraph (b))

The Commission proposes to streamline § 312.4(b),¹⁰⁸ regarding the placement and content of the notice of information practices that operators must provide on their Web sites or in their online services. The language regarding the required placement of this online notice has been shortened and clarified, thereby making the provision more instructive to operators. The

¹⁰⁵ See 1999 Statement of Basis and Purpose, 64 FR 59888, 59897.

¹⁰⁶ See Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 57–59.

¹⁰⁷ The proposed changes to the direct notice provision, discussed in Part V.B.(2) *infra*, would reverse the Commission's guidance that operators may truncate the information in the direct notice by providing a hyperlink to their online privacy policy. See note 105 and accompanying text.

¹⁰⁸ No changes are proposed to § 312.4(a) ("general principles of notice").

revised language more succinctly requires that the online notice be clearly labeled and prominently located, and be posted on an operator's home page or home screen and at each location where the operator collects personal information from children.¹⁰⁹

With respect to the content of the online notice, the Commission proposes several improvements to the Rule's current list of requirements. First, the Commission proposes requiring operators to provide contact information, including, at a minimum, the operator's name, physical address, telephone number, and e-mail address. In contrast to the current Rule, this proposal would apply to *all* operators of a Web site or online service, rather than permitting the designation of a single operator as the contact point. Given the possibility of a child interacting with multiple operators on a single Web site or online service (*e.g.*, in the case of a mobile application that grants permission to an advertising network to collect user information from within the application), the Commission believes that the identification of each operator will aid parents in finding the appropriate party to whom to direct any inquiry.

Second, the Commission proposes eliminating the Rule's current lengthy—yet potentially under-inclusive—recitation of an operator's information collection, use, and disclosure practices in favor of a simple statement of: (1) What information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available, (2) how the operator uses such information, and (3) the operator's disclosure practices for such information.¹¹⁰ In the Commission's experience, privacy policies are often long and difficult to understand, and may no longer be the most effective way to communicate salient information to consumers, including parents.¹¹¹ By streamlining the Rule's online notice requirements by reverting to the language of the COPPA statute, the Commission hopes to encourage operators to provide clear, concise descriptions of their information practices, which may have the added benefit of being easier to read on smaller

¹⁰⁹ The Commission poses a question whether the Rule should be modified to require operators to post a link to their online notice in any location where their mobile applications can be purchased or otherwise downloaded. See *infra* Part X. at Question 14.

¹¹⁰ This language mirrors the statutory requirements for the online notice. See 15 U.S.C. 6503(b)(1)(A)(i).

¹¹¹ See Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 7.

screens (*e.g.*, those on Internet-enabled mobile devices).

The Commission also proposes eliminating the requirement, articulated in § 312.4(b)(2)(v), that an operator's privacy policy state that the operator may not condition a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. In the Commission's experience, this blanket statement, often parroted verbatim in operators' privacy policies, detracts from the key information of operators' actual information practices, and yields little value to a parent trying to determine whether to permit a child's participation. In proposing to delete this requirement in the privacy notice, however, the Commission does not propose deleting § 312.7 of the Rule, which still prohibits operators from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.¹¹²

Therefore, the Commission proposes to revise paragraph (b) of § 312.4 so that it states:

(b) *Notice on the Web site or online service.* Pursuant to § 312.3(a), each operator of a Web site or online service directed to children must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and*, at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) Each operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and e-mail address;

(2) A description of what information each operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,

(3) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of

¹¹² See 16 CFR 312.7.

the child's information, and state the procedures for doing so.¹¹³

(2) Direct Notice to a Parent (Revised Paragraph (c))

As described above, the Commission proposes refining the Rule requirements for the direct notice to ensure that this notice works as an effective "just-in-time" message to parents about an operator's information practices. Specifically, the Commission proposes to reorganize and standardize the direct notice requirement to set forth the precise items of information that must be disclosed in each type of direct notice required under the Rule. These specific notice requirements correspond to the requirements for obtaining parental consent under § 312.5 of the Rule. The proposed reorganization is intended to make it easier for operators to determine what information they must include in the direct notice to parents, based upon operators' particular information collection practices.

The proposed revised language of § 312.4(c) specifies, for each different form of direct notice required by the Rule, the precise information that operators must provide to parents regarding: The items of personal information the operator already has obtained from the child (the parent's online contact information either alone or together with the child's online contact information); the purpose of the notification; action that the parent must or may take; and, what use, if any, the operator will make of the personal information collected. The proposed revised provision also makes clear that each form of direct notice must provide a hyperlink to the operator's online notice of information practices. The Commission believes the proposed revisions will help ensure that parents receive key information up front, while directing them online to view any additional information contained in the operator's online notice.

The Commission also proposes adding a new paragraph, § 312.4(c)(2),

¹¹³No change is proposed to the Rule's requirement that operators disclose that a parent may review and have deleted a child's personal information and refuse to permit further collection or use of that child's information. Although one commenter observed that parents seldom exercise these rights, see *WiredSafety.org* (comment 68), at 28, the Commission believes that requiring operators to provide such rights to parents remains an important element of the Rule. In the context of its broader inquiry into how to best protect privacy in today's marketplace, Commission staff is exploring methods of ensuring consumer access to data as a means of increasing the transparency of companies' data practices. See *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 23, at 72-76.

setting out the requirements for a direct notice when an operator chooses to collect a parent's online contact information from the child in order to provide parental notice about a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. This new form of parental notice corresponds to a newly proposed exception to the parental consent requirement for the collection of a parent's online contact information when done to inform the parent of a child's participation in a Web site or online service that does not otherwise collect personal information from the child.¹¹⁴

Therefore, the Commission proposes to revise paragraph (c) of § 312.4 so that it reads:

(c) *Direct notice to a parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of the child's personal information, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(1) *Content of the direct notice to the parent required under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information).* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to obtain the parent's consent;

(ii) That the parent's consent is required for the child's participation in the Web site or online service, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, if any, and the potential opportunities for the disclosure of personal information, if any, should the parent consent to the child's participation in the Web site or online service;

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b);

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and,

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) *Content of the direct notice to the parent allowed under § 312.5(c)(2) (Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the

child in order to provide notice to the parent of a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information; and,

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the operator to allow the child to participate in the Web site or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and,

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(3) *Content of the direct notice to the parent required under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times).* This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and,

(vi) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety).* This direct notice shall set forth:

(i) That the operator has collected the child's name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and,

(v) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

C. Parental Consent (16 CFR 312.5)

A central element of COPPA is its requirement that operators seeking to collect, use, or disclose personal

¹¹⁴ See *infra* Part V.C.(4).

information from children first obtain verifiable parental consent.¹¹⁵ “Verifiable parental consent” is defined in the statute as “any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure, described in the notice.”¹¹⁶ In paragraph (b)(1), the Rule provides that operators:

must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated in light of available technology to ensure that the person providing consent is the child’s parent.

The Rule then sets forth a non-exclusive list of methods that meet the standard of verifiable parental consent.¹¹⁷ Specifically, paragraph (b)(2) states:

Methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: Providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph.¹¹⁸

The Rule’s enumerated consent mechanisms were discussed in-depth at the Commission’s June 2, 2010 COPPA roundtable and also were addressed by

¹¹⁵ Paragraph (a) of § 312.5 reads:

(1) An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child’s personal information without consenting to disclosure of his or her personal information to third parties.

¹¹⁶ 15 U.S.C. 6501(9).

¹¹⁷ See 16 CFR 312.5(b).

¹¹⁸ Paragraph (b)(2) continues:

Provided that: Until the Commission otherwise determines, methods to obtain verifiable parental consent for uses of information other than the “disclosures” defined by § 312.2 may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent’s consent by letter or telephone call. Operators who use such methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.

A discussion of paragraph (b)(2) follows in Part V.C.(2).

a number of commenters.¹¹⁹ While several persons acknowledged that no one method provides complete certainty that the operator has reached and obtained consent from a parent, they generally agreed that the listed methods continue to have utility for operators and should be retained.¹²⁰ A great number of commenters also urged the Commission to expand the list of acceptable mechanisms to incorporate newer technologies.¹²¹ After careful consideration, the Commission proposes several significant changes to the mechanisms of verifiable parental consent set forth in paragraph (b) of § 312.5, including: Adding several newly recognized mechanisms for parental consent; eliminating the sliding scale approach to parental consent; and, adding two new processes for evaluation and pre-clearance of parental consent mechanisms.

(1) Mechanisms for Verifiable Parental Consent (Paragraph (b)(2))

A number of commenters made suggestions for strengthening, modernizing, and simplifying the Rule’s mechanisms for parental consent. For example, commenters asked the Commission to recognize additional methods of obtaining parental consent, such as by sending a text message to the parent’s mobile phone number,¹²² offering online payment services other than credit cards,¹²³ offering parental controls in gaming consoles,¹²⁴ offering a centralized parents’ opt-in list,¹²⁵ and

¹¹⁹ See Federal Trade Commission’s Roundtable: Protecting Kids’ Privacy Online at 195, 208–71 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

¹²⁰ See DMA (comment 17), at 10, 12; Microsoft (comment 39), at 7; Toy Industry Association, Inc. (comment 63), at 3; WiredSafety.org. (comment 68), at 18.

¹²¹ See, e.g., Boku (comment 5); DMA (comment 17), at 11–12; EchoSign, Inc. (comment 18); Entertainment Software Association (comment 20), at 7–9; Facebook (comment 22), at 2; Janine Hiller (comment 27), at 447–50; Mary Kay Hoal (comment 30); Microsoft (comment 39), at 4; MPAA (comment 42), at 12; RelyID (comment 53), at 3; TRUSTe (comment 64), at 3; Harry Valetk (comment 66), at 6; WiredSafety.org (comment 68), at 53; Susan Wittlief (comment 69).

¹²² See BOKU (comment 5); Entertainment Software Association (comment 20), at 11–12; TRUSTe (comment 64), at 3; Harry A. Valetk (comment 66), at 6–7. See discussion *supra* Part IV, regarding COPPA’s application to mobile communications via SMS messaging.

¹²³ See WiredSafety.org (comment 68), at 24 (noting that operators are considering employing online financial accounts such as iTunes for parental consent).

¹²⁴ See Entertainment Software Association (comment 20), at 9–10; Microsoft (comment 39), at 7.

¹²⁵ See Entertainment Software Association (comment 20), at 12; Janine Hiller (comment at 27), at 31.

permitting electronic signatures.¹²⁶ Upon consideration of each proposal in light of the existing record, the Commission determines that the record is sufficient to justify certain proposed mechanisms, but insufficient to adopt others.

First, the Commission notes that the collection of a parent’s mobile phone number to effectuate consent via an SMS text message would require a statutory change, as the COPPA statute currently permits only the collection of a parent’s “online contact” information for such purposes, and a phone number does not fall within the statute’s definition of “online contact information,” *i.e.*, “an e-mail address or another substantially similar identifier that permits direct contact with a person online.”¹²⁷ There are advantages to using SMS texting as a method of contacting the parent and obtaining consent—among them that parents typically do not have multiple mobile phone numbers, and generally have their mobile phones with them at all times. Some commenters opined that this method was as reliable as use of a credit card or fax;¹²⁸ others compared the use of SMS text messaging to the “e-mail plus” method permitted under the Rule’s sliding scale approach to parental consent.¹²⁹ The Commission believes the more apt analogy is to the e-mail plus method in that the operator sends a notice to the parent via the parent’s mobile phone number and requests opt-in consent by a return message in some form. In this way, the use of SMS text messaging for parental consent would suffer from the same inadequacies as does e-mail plus, which, as described below, the Commission proposes to eliminate. Just as with an e-mail address, there is no way to verify that the phone number provided by a child is that of the parent rather than that of the child. For these reasons, the Commission declines to add use of SMS text messaging to the enumerated list of parental consent mechanisms.

With respect to expanding the Rule to permit the use of online payment services for verifying consent in lieu of a credit card, the Commission finds that the record is insufficient to warrant adding online payment services as a consent mechanism. The Commission notes that no commenters provided any

¹²⁶ See DMA (comment 17), at 12; EchoSign (comment 18); Entertainment Software Association (comment 20), at 10; Toy Industry Association (comment 63), at 11.

¹²⁷ 15 U.S.C. 6502(12).

¹²⁸ See, e.g., Entertainment Software Association (comment 20), at 11–12.

¹²⁹ See Boku (comment 5).

analysis of how online payment services might meet the requirements of § 312.5(b)(1); however, one commenter cautioned the Commission against embracing such technologies at this time, noting that alternative payment systems may not be as well-regulated as the credit card industry and thereby may provide even less assurance of parental consent than use of a credit card.¹³⁰ The Commission also is mindful of the potential for children's easy access to and use of alternative forms of payments (such as gift cards, debit cards, and online accounts), and would expect to see a fuller discussion of the risks presented in any future application to the Commission for recognition of these consent methods.

Several commenters asked the Commission to consider whether, and in what circumstances, parental control features in game consoles could be used to verify consent under COPPA.¹³¹ Parental control settings often permit parents to limit or block functions such as Internet access, information sharing, chat, and interactive game play, and require parental approval before a child adds friends.¹³² Parental control features appear to offer parents a great deal of control over a child's gaming experience, and, as commenters acknowledged, can serve as a *complement* to COPPA's parental consent requirements.¹³³ As acknowledged in the comments, at present, such systems are not designed to comply with COPPA's standards for verifiable parental consent,¹³⁴ and the record currently is insufficient for the Commission to determine whether a hypothetical parental consent mechanism would meet COPPA's verifiable parental consent standard. The Commission encourages continued exploration of the concept of using parental controls in gaming consoles (and, presumably, on a host of handheld devices) to notify parents and obtain their prior verifiable consent.

¹³⁰ See EPIC (comment 19), at 5. ("Alternative methods may not be as heavily regulated as more traditional systems. As a result, the use of alternative methods in gaining parental consent or payment remain inadvisable, although that may change as such methods come under stronger regulation.")

¹³¹ See Entertainment Software Association (comment 20), at 4; Microsoft (comment 39), at 7.

¹³² See Entertainment Software Association (comment 20), at 4–6.

¹³³ *Id.* at 6.

¹³⁴ See *id.* at 9 ("Therefore, it makes sense to consider how these tools could be harnessed for the related task of acquiring verifiable parental consent under the COPPA Rule"); Microsoft (comment 39), at 7 (describing how a hypothetical parental controls method might be structured in the future to notify a parent and obtain parental consent).

Several commenters also asked the Commission to accept electronic signatures as a form of verifiable consent.¹³⁵ The term "electronic signature" has many meanings, and can range from "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record,"¹³⁶ to an electronic image of the stylized script associated with a person. Although the law recognizes electronic signatures for the assertion that a document has been signed,¹³⁷ electronic signatures do not necessarily confirm the underlying identity of the individual signing the document. Therefore, their use, without more indicia of reliability, is problematic in the context of COPPA's verifiable parental consent requirement.

The Entertainment Software Association proposed that the Commission incorporate a "sign and send" method, given that Internet-enabled mobile devices increasingly include technologies that allow a user to input data by touching or writing on the device's screen. The Commission agrees that such sign-and-send methods are substantially analogous to the print-and-send method already recognized by § 312.5(b)(2) of the Rule.¹³⁸ However, because of the proliferation of mobile devices among children and the ease with which children could sign and return an on-screen consent, the Commission is concerned that such mechanisms may not "ensure that the person providing consent is the child's parent."¹³⁹ The Commission welcomes further comment on how to enhance the reliability of these convenient methods.

Several commenters urged the Commission to recognize the submission of electronically scanned versions of signed parental consent forms and the use of video verification methods.¹⁴⁰ The Commission agrees that now commonly-available

¹³⁵ See DMA (comment 17), at 12; EchoSign (comment 18); Entertainment Software Association (comment 20), at 10; Toy Industry Association (comment 63), at 11.

¹³⁶ See Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7006(5).

¹³⁷ 15 U.S.C. 7001(a).

¹³⁸ See Entertainment Software Association (comment 20), at 10.

¹³⁹ 16 CFR 312.5(b)(1).

¹⁴⁰ See Denise Tayloe, *supra* note 42, at 227; Phyllis B. Spaeth, Assoc. Dir., Children's Adver. Review Unit, Council of Better Bus. Bureaus, Remarks from *The "Actual Knowledge" Standard in Today's Online Environment* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 269 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf; DMA (comment 17), at 11; EPIC (comment 19), at 3.

technologies such as electronic scans and video conferencing are functionally equivalent to the written and oral methods of parental consent originally recognized by the Commission in 1999. Therefore, the Commission proposes to recognize these two methods in the proposed Rule.

The Commission also proposes allowing operators to collect a form of government-issued identification—such as a driver's license, or a segment of the parent's social security number—from the parent, and to verify the parent's identity by checking this identification against databases of such information, provided that the parent's identification is deleted by the operator from its records promptly after such verification is complete. The Commission recognizes that information such as social security number, driver's license number, or other record of government-issued identification are sensitive data.¹⁴¹ In permitting operators to use government-issued identification as an approved method of parental verification, the Commission emphasizes the importance of limiting the collection of such identification information to only those segments of information needed to verify the data.¹⁴² For example, the Commission notes that the last four digits of a person's social security number are commonly used by verification services to confirm a person's identity.¹⁴³ The requirement in the proposed Rule that operators immediately delete parents' government-issued identification information upon completion of the verification process provides further protection against operators' unnecessary retention of the information, use of the information for

¹⁴¹ The COPPA statute itself lists social security number among the items considered to be personal information. See 16 CFR 312.2. In other contexts, driver's licenses and social security numbers, among other things, have traditionally been considered by Commission staff to be personal, or sensitive, as well. See Self-Regulatory Principles for Online Behavioral Advertising, *supra* note 68, at 20, 42, 44.

¹⁴² The use of a driver's license to verify a parent, while not specifically enumerated in the Final Rule as an approved method of parental consent, was addressed in the Statement of Basis and Purpose in connection with a discussion of the methods to verify the identity of parents who seek access to their children's personal information under § 312.6(a)(3) of the Rule. See 1999 Statement of Basis and Purpose, 64 FR 59888, 59905. There, the Commission concluded that the use of a driver's license was an acceptable method of parental verification.

¹⁴³ See, e.g., Privo, Inc., "Request for Safe Harbor Approval by the Federal Trade Commission for Privo, Inc.'s Privacy Assurance Program under Section 312.10 of the Children's Online Privacy Protection Rule," 25 (Mar. 3, 2004), available at <http://www.ftc.gov/os/2004/04/privoapp.pdf>.

other purposes, and potential compromise of such information.¹⁴⁴

Finally, the Commission proposes including the term “monetary” to modify “transaction” in connection with use of a credit card to verify parental consent. This added language is intended to make clear the Commission’s long-standing position that the Rule limits use of a credit card as a method of parental consent to situations involving actual monetary transactions.¹⁴⁵

(2) The Sliding Scale Approach to Parental Consent

In conducting the Rule review, the Commission sought comment on whether the sliding scale set forth in § 312.5(b)(2) remains a viable approach to verifiable parental consent.¹⁴⁶ Under the sliding scale, an operator, when collecting personal information only for its *internal* use, may obtain verifiable parental consent through an e-mail from the parent, so long as the e-mail is coupled with an additional step. Such additional steps have included: Obtaining a postal address or telephone number from the parent and confirming the parent’s consent by letter or telephone call, or sending a delayed confirmatory e-mail to the parent after receiving consent. The purpose of the additional step is to provide greater assurance that the person providing consent is, in fact, the parent.¹⁴⁷ This consent method is often called “email plus.” In contrast, for uses of personal information that involve disclosing the information to the public or third parties, the sliding scale approach requires operators to use more reliable methods of obtaining verifiable parental consent. These methods have included: Using a print-and-send form that can be

faxed or mailed back to the operator; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the above methods.

In adopting the sliding scale approach in 1999, the Commission recognized that the e-mail plus method was not as reliable as the other enumerated methods of verifiable parental consent.¹⁴⁸ However, it believed that this lower cost option was acceptable as a temporary option, in place only until the Commission determined that more reliable (and affordable) consent methods had adequately developed.¹⁴⁹ In 2006, the Commission extended use of the sliding scale indefinitely, stating that the agency would continue to monitor technological developments and modify the Rule should an acceptable electronic consent technology develop.¹⁵⁰

E-mail plus has enjoyed wide appeal among operators, who credit its simplicity.¹⁵¹ Numerous commenters, including associations who represent operators, support the continued retention of this method as a low-cost means to obtain parents’ consent.¹⁵² At the same time, several commenters, including safe harbor programs and proponents of new parental consent mechanisms, challenged the method’s reliability, given that operators have no

real way of determining whether the e-mail address provided by a child is that of the parent, and there is no requirement that the parent’s e-mail response to the operator contain any additional information providing assurance that it is from a parent.¹⁵³

The Commission believes that the continued reliance on e-mail plus has inhibited the development of more reliable methods of obtaining verifiable parental consent.¹⁵⁴ In fact, the Commission notes that few, if any, new methods for obtaining parental consent have emerged since the sliding scale was last extended in 2006. The Commission limited the use of e-mail plus to instances where operators only collect children’s personal information for internal uses. Although internal uses may pose a lower risk of misuse of children’s personal information than the sharing or public disclosure of such information, all collections of children’s information merit strong verifiable parental consent. Indeed, children’s personal information is one of the most sensitive types of data collected by operators online. In light of this, therefore, the Commission believes that e-mail plus has outlived its usefulness and should no longer be a recognized approach to parental consent under the Rule.

Therefore, the Commission proposes to amend § 312.5(b)(2) so that it reads:

(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or an electronic scan; permitting a parent to use a credit card in connection with a monetary transaction; having a parent call a toll-free telephone number staffed by trained personnel; having a parent connect to trained personnel via video-conference; or, verifying a parent’s identity by checking a form of government-issued identification against databases of such information, *provided that* the parent’s identification is deleted by the operator from its records promptly after such verification is complete.

¹⁵³ See Privo, Inc. (comment 50), at 5 (“the presentation of a verified email is much less reliable if there is virtually no proofing or analyzing that goes on to determine who the email belongs to”); RelyId (comment 53), at 3 (“The email plus mechanism does not obtain verifiable parental consent at all. It simply does not ensure that a parent ‘authorizes’ anything required by the COPPA statute. The main problem with this approach is that the child can create an email address to act as the supposed parent’s email address, send the email from that address, and receive the confirmatory email at that address”). See also Denise Tayloe, *supra* note 42, at 215–17; Phyllis Spaeth, *supra* note 140, at 215–17 (e-mail plus is very unreliable).

¹⁵⁴ See Privo (comment 50), at 4 (“[E]xtending the sliding scale mechanism had the effect of giving industry absolutely no reason to create, innovate, adopt or make use of any other method for the internal use of children’s personal data.”)

¹⁴⁴ The Commission poses a question whether operators should be required to maintain a record that parental consent was obtained. See *infra* Part X., at Question 17.

¹⁴⁵ See Children’s Online Privacy Protection Rule, 71 FR 13247, 13253, 13254 (Mar. 15, 2006) (retention of rule without modification) (requirement that the credit card be used in connection with a transaction provides extra reliability because parents obtain a transaction record, which is notice of the purported consent, and can withdraw consent if improperly given); Fed. Trade Comm’n., Frequently Asked Questions about the Children’s Online Privacy Protection Rule, Question 33, available at <http://www.ftc.gov/privacy/coppafaqs.shtm#consent>.

¹⁴⁶ See 2010 Rule Review, *supra* note 7, at 17091.

¹⁴⁷ The Commission was persuaded by commenters’ views that internal uses of information, such as marketing to children, presented less risk than external disclosures of the information to third parties or through public postings. See 1999 Statement of Basis and Purpose, 64 FR 59888, 59901. Other internal uses of children’s personal information may include sweepstakes, prize promotions, child-directed fan clubs, birthday clubs, and the provision of coupons.

¹⁴⁸ See *id.* at 59,902 (“[E]mail alone does not satisfy the COPPA because it is easily subject to circumvention by children.”).

¹⁴⁹ See *id.* at 59,901 (“The Commission believes it is appropriate to balance the costs imposed by a method against the risks associated with the intended uses of the information collected. Weighing all of these factors in light of the record, the Commission is persuaded that temporary use of a “sliding scale” is an appropriate way to implement the requirements of the COPPA until secure electronic methods become more available and affordable”).

¹⁵⁰ See Children’s Online Privacy Protection Rule, 71 FR 13247, 13255, 13254 (Mar. 15, 2006) (retention of rule without modification).

¹⁵¹ See WiredSafety.org (comment 68), at 21 (“We all assumed [email plus] would be phased out once digital signatures became broadly used. But when new authentication models and technologies failed to gain in parental adoption, it was continued and is in broad use for one reason—it’s simple”).

¹⁵² See Rebecca Newton, Chief Cmty. & Safety Officer, Mind Candy, Inc., Remarks from *Emerging Parental Verification Access and Methods* Panel at the Federal Trade Commission’s Roundtable: Protecting Kids’ Privacy Online at 211–13 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf (e-mail plus is as reliable as any other method); DMA (comment 17), at 10; IAB (comment 34), at 2; Rebecca Newton (comment 46), at 3; PMA (comment 51), at 4–5; Toy Industry Association, Inc. (comment 63), at 8.

However, as explained below, given the proposed discontinuance of e-mail plus, and in the interest of spurring innovation in parental consent mechanisms, the Commission proposes a new process by which parties may voluntarily seek Commission approval of a particular consent mechanism, as explained below.

(3) Commission and Safe Harbor Approval of Parental Consent Mechanisms (New Paragraphs (b)(3) and (b)(4))

Under the Rule, methods to obtain verifiable parental consent “must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.”¹⁵⁵ This standard provides operators with the opportunity to craft consent mechanisms that meet this standard but otherwise are not enumerated in paragraph (b)(2) of § 312.5. Nevertheless, whether out of concern for potential liability, ease of implementation, or lack of technological developments, operators have been reluctant to utilize consent methods other than those specifically set forth in the Rule.¹⁵⁶ As a result, there appears to be little technical innovation in any area of parental consent.¹⁵⁷

To encourage the development of new consent mechanisms, and to provide transparency regarding consent mechanisms that may be proposed, the Commission proposes to establish a process in the Rule through which parties may, on a voluntary basis, seek Commission approval of a particular consent mechanism. Applicants who seek such approval would be required to present a detailed description of the proposed parental consent mechanism, together with an analysis of how the mechanism meets the requirements of § 312.5(b)(1) of the Rule. The Commission would publish the application in the **Federal Register** for public comment, and approve or deny the applicant’s request in writing within 180 days of the filing of the request.

¹⁵⁵ See 16 CFR 312.5(b)(1).

¹⁵⁶ The June 2, 2010 Roundtable and the public comments reflect a tension between operators’ desire for new methods of parental verification and their hesitation to adopt consent mechanisms other than those specifically enumerated in the Rule. See Remarks from Federal Trade Commission’s Roundtable: Protecting Kids’ Privacy Online at 226–27 (June 2, 2010), available at http://www.ftc.gov/bcp/workshops/coppa/vCOPPARuleReview_Transcript.pdf; CDT (comment 8), at 3 (“innovation in developing procedures to obtain parental consent has been limited as websites choose to use the methods suggested by the FTC out of fear that a more innovative method could lead to liability”).

¹⁵⁷ See Children’s Online Privacy Protection Rule, 71 FR 13247, 13250 (Mar. 15, 2006) (retention of rule without modification).

The Commission believes that this new approval process, aided by public input, will allow the Commission to give careful consideration, on a case-by-case basis, to new forms of consent as they develop in the marketplace. The new process also will increase transparency by publicizing approvals or rejections of particular consent mechanisms and should encourage operators who may previously have been tentative about exploring technological advancements to come forward and share them with the Commission and the public.

Several commenters urged the Commission to permit Commission-approved safe harbor programs to serve as laboratories for developing new consent mechanisms.¹⁵⁸ The Commission agrees that establishing such a system may aid the pace of development in this area, and given the strengthened oversight of safe harbor programs described in Part F. below, will not result in the loosening of COPPA’s standards for parental consent. Therefore, the Commission proposes adding a provision to the Rule stating that operators participating in a Commission-approved safe harbor program may use any parental consent mechanism deemed by the safe harbor program to meet the general consent standard set forth in § 312.5(b)(1).

Therefore, the Commission proposes to amend § 312.5(b) to add two new paragraphs, (3) and (4) that read:

(3) *Commission approval of parental consent mechanisms.* Interested parties may file written requests for Commission approval of parental consent mechanisms not currently enumerated in paragraph (b)(2). To be considered for approval, parties must provide a detailed description of the proposed parental consent mechanism, together with an analysis of how the mechanism meets paragraph (b)(1). The request shall be filed with the Commission’s Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 180 days of the filing of the request.

(4) *Safe harbor approval of parental consent mechanisms.* A safe harbor program approved by the Commission under § 312.11 may approve its member operators’ use of a parental consent mechanism not currently enumerated in paragraph (b)(2) where the safe harbor program determines that such parental consent mechanism meets the requirements of paragraph (b)(1).

¹⁵⁸ See MPAA (comment 42), at 12; Rebecca Newton (comment 46), at 2; Privo (comment 50), at 2; PMA (comment 51), at 5; Berin Szoka (comment 59), Szoka Responses to Questions for the Record, at 56; TRUSTe (comment 64), at 3. See also generally WiredSafety.org (comment 68), at 31–32.

(4) Exceptions to Prior Parental Consent (Paragraph (c))

Congress anticipated that certain situations would arise in which it was not necessary or practical for an operator to obtain consent from parents prior to engaging with children online. Accordingly, the COPPA statute and Rule contain five scenarios in which an operator may collect limited pieces of personal information (*i.e.*, name and online contact information) from children prior to, or sometimes without, obtaining consent.¹⁵⁹ These exceptions permit operators to communicate with the child to: initiate the parental consent process, respond to the child once or multiple times, and protect the child’s safety or the integrity of the Web site.¹⁶⁰

The Commission proposes adding one new exception to parental consent in order to give operators the option to collect a parent’s online contact information for the purpose of providing notice to or updating the parent about a child’s participation in a Web site or online service that does not otherwise collect, use, or disclose children’s personal information.¹⁶¹ The parent’s online contact information may not be used for any other purpose, disclosed, or combined with any other information collected from the child. The Commission believes that collecting a parent’s online contact information for the limited purpose of notifying the parent of a child’s online activities in a site or service that does not otherwise collect personal information is reasonable and should be encouraged.¹⁶²

Therefore, the Commission proposes to amend § 312.5(c) to add a new subsection, § 312.4(c)(2), that reads:

Where the sole purpose of collecting a parent’s online contact information is to provide notice to, and update the parent about, the child’s participation in a Web site or online service that does not otherwise collect, use, or disclose children’s personal information. In such cases, the parent’s online contact information may not be used

¹⁵⁹ See 15 U.S.C. 6503(b)(2); 16 CFR 315.5(c).

¹⁶⁰ The Act and the Rule currently permit the collection of a parent’s e-mail address for the limited purposes of: (1) obtaining verified parental consent; (2) providing parents with a right to opt-out of an operator’s use of a child’s e-mail address for multiple contacts of the child; and (3) to protect a child’s safety on a Web site or online service. See 15 U.S.C. 6503(b)(2); 16 CFR 312.5(c)(1), (2), and (4).

¹⁶¹ At least a few online virtual worlds directed to very young children already follow this practice. Because the Rule does not currently include such an exception, these operators technically are in violation of COPPA.

¹⁶² This proposed new exception is mirrored in the proposed revisions to the direct notice requirement of § 312.4. See *supra* Part V.B.(2).

or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2).

The Commission also proposes minor technical corrections to the Rule's current exceptions provisions. First, in § 312.4(c)(1), the Rule permits an operator to collect "the name or online contact information of a parent or child" to be used for the sole purpose of obtaining parental consent. The clear intent of this provision is to allow for the collection of the *parent's* online contact information in order to reach the parent to initiate the consent process. Therefore, the Commission proposes to amend § 312.5(c)(1) to clarify the language so that it reads:

Where the sole purpose of collecting a parent's online contact information and the name of the child or the parent is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records.

Second, § 312.5(c)(3) provides that an operator may notify a parent of the collection of a child's online contact information for multiple contacts via e-mail or postal address. The Commission proposes to eliminate the option of collecting a parent's postal address for notification purposes. The collection of postal address is not provided for anywhere else in the Rule's notice requirements, and is clearly outmoded at this time. Therefore, the Commission proposes to amend § 312.5(c)(3), now renumbered as § 312.5(4), so that it reads:

Where the sole purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered.

Finally, in various places in § 312.5(c), the Commission proposes to emphasize that the collection of online contact information is to be used for the limited purpose articulated within each paragraph, and not for any other purpose.

Therefore, the Commission proposes to amend § 312.5(c) so that it reads in its entirety:

(c) *Exceptions to prior parental consent.* Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in this paragraph:

(1) Where the sole purpose of collecting a parent's online contact information and the name of the child or the parent is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the sole purpose of collecting a parent's online contact information is to provide notice to, and update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting a child's online contact information is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;¹⁶³

(4) Where the sole purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the sole purpose of collecting a child's name, and a child's and a parent's online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the sole purpose of collecting a child's name and online contact information is to: (i) Protect the security or integrity of its Web site or online service; (ii) take precautions against liability; (iii) respond to judicial process; or (iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and, where such

¹⁶³ This "one time use" exception does not require an operator to provide notice to a parent.

information is not be used for any other purpose.¹⁶⁴

D. Confidentiality, Security, and Integrity of Personal Information Collected From Children (16 CFR 312.8)

The Commission proposes to amend § 312.8 to strengthen the provision for maintaining the confidentiality, security, and integrity of personal information. To accomplish this, the Commission proposes adding a requirement that operators take reasonable measures to ensure that any service provider or third party to whom they release children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

COPPA requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, but is silent on the data security obligations of third parties.¹⁶⁵ The COPPA Rule mirrors the statutory language but also requires covered operators to disclose in their online privacy policies whether third parties to whom personal information is disclosed have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator.¹⁶⁶

Under the Commission's proposed amendment to § 312.8, an operator must take reasonable measures to ensure that any service provider or third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information. This provision is intended to address security issues surrounding business-to-business releases of data.¹⁶⁷

The proposed requirement that operators must take reasonable measures to ensure that third parties and service providers keep the shared information confidential and secure is a logical and necessary extension of the statutory requirement that operators themselves keep such information confidential and secure. Therefore, the Commission proposes to amend § 312.8 to add a second sentence so that it reads:

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must take reasonable measures

¹⁶⁴ This exception does not require an operator to provide notice to a parent.

¹⁶⁵ 15 U.S.C. 6503(b)(1)(D).

¹⁶⁶ See 16 CFR 312.4(b)(2)(iv) and 312.8.

¹⁶⁷ See *supra* Part V.A.(3).

to ensure that any service provider or any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

E. Data Retention and Deletion Requirements (Proposed 16 CFR 312.10)

As noted above, COPPA authorizes the Commission to promulgate regulations requiring operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.¹⁶⁸ Deleting unneeded information is an integral part of any reasonable data security strategy. Accordingly, the Commission proposes adding a new data retention and deletion provision to become § 312.10.¹⁶⁹

The proposed provision states that operators shall retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. In addition, it states that an operator must delete such information by taking reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

Although the current Rule does not contain a data retention and deletion requirement, the Commission has long encouraged such practices. According to its 1999 Notice of Proposed Rulemaking: “[t]he Commission encourages operators to establish reasonable procedures for the destruction of personal information once it is no longer necessary for the fulfillment of the purpose for which it was collected. Timely elimination of data is the ultimate protection against misuse or unauthorized disclosure.”¹⁷⁰ More recently, the Commission has testified that companies should adopt a “privacy by design” approach, including by building data retention and disposal protections into their everyday business practices.¹⁷¹

¹⁶⁸ 15 U.S.C. 6503(b)(1)(D).

¹⁶⁹ The Commission proposes moving the current § 312.10 (Safe Harbors) to § 312.11, and deleting as obsolete the current § 312.11 (Rulemaking review).

¹⁷⁰ See Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 64 FR 22750, 22758–59 (Apr. 27, 1999), available at <http://www.ftc.gov/os/fedreg/1999/april/990427childrensonlineprivacy.pdf>.

¹⁷¹ See, e.g., *Internet Privacy: The Views of the FTC, the FCC, and NTIA: Hearing Before the Subcomm. on Commerce, Manufacturing, & Trade and Communications & Technology of the H.R. Comm. on Energy and Commerce*, 112th Cong., at 14 (2011) (Statement of Edith Ramirez, Commissioner, Federal Trade Commission), available at <http://www.ftc.gov/os/testimony/110714internetprivacytestimony.pdf>; *Privacy and Data Security: Protecting Consumers in the Modern*

The proposed new data retention and deletion provision (§ 312.10) reads:

An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

F. Safe Harbors (Current 16 CFR 312.10, Proposed 16 CFR 312.11)

The COPPA statute established a “safe harbor” for participants in Commission-approved COPPA self-regulatory programs.¹⁷² With the safe harbor provision, Congress intended to encourage industry members and other groups to develop their own COPPA oversight programs, thereby promoting efficiency and flexibility in complying with COPPA's substantive provisions.¹⁷³ COPPA's safe harbor provision also was intended to reward operators' good faith efforts to comply with COPPA. The Rule therefore provides that operators fully complying with an approved safe harbor program will be A “deemed to be in compliance” with the Rule for purposes of enforcement. In lieu of formal enforcement actions, such operators instead are subject first to the safe harbor program's own review and disciplinary procedures.¹⁷⁴

Current § 312.10 of the Rule sets forth the criteria the Commission uses to approve applications for safe harbor status under COPPA. First, the self-regulatory program must contain guidelines that protect children's online privacy to the same or greater extent as the Rule and ensure that each potential participant complies with these

World: Hearing Before the S. Comm. on Commerce, Science & Transportation, 112th Cong., at 12 (2011) (Statement of Julie Brill, Commissioner, Federal Trade Commission), available at <http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf>; *Data Security: Hearing Before the Subcomm. on Commerce, Manufacturing & Trade, H.R. Comm. on Energy and Commerce*, 112th Cong., at 9 (2011) (Statement of Edith Ramirez, Commissioner, Federal Trade Commission), available at <http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf>. See also Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 44.

¹⁷² See 15 U.S.C. 6503.

¹⁷³ See 1999 Statement of Basis and Purpose, 64 FR 59888, 59906 (“[T]his section serves as an incentive for industry self-regulation; by allowing flexibility in the development of self-regulatory guidelines, it ensures that the protections afforded children under this Rule are implemented in a manner that takes into account industry specific concerns and technological developments”).

¹⁷⁴ See 16 CFR 312.10(a) and (b)(4).

guidelines.¹⁷⁵ Second, the program must monitor the participant's practices on an ongoing basis to ensure that the participant continues to comply with both the program's guidelines and the participant's own privacy notices.¹⁷⁶ Finally, the safe harbor program must contain effective incentive mechanisms to ensure operators' compliance with program guidelines.¹⁷⁷

Several comments supported strengthening the Commission's oversight of participating safe harbor programs. TRUSTe, a Commission-approved COPPA safe harbor program, asked the Commission to develop better criteria for the approval of safe harbor programs that reflect the principles of reliability, accountability, transparency, and sustainability.¹⁷⁸ Another commenter urged the Commission regularly to audit the Commission-approved COPPA safe harbor programs to ensure compliance with the Rule.¹⁷⁹ The Commission finds merit in the calls to strengthen the Safe Harbor provisions of the Rule, and accordingly, proposes three substantive changes: requiring that applicants seeking Commission approval of self-regulatory guidelines submit comprehensive information about their capability to run an effective safe harbor program; establishing more rigorous baseline oversight by Commission-approved safe harbor programs of their members; and, requiring Commission-approved safe harbor programs to submit periodic reports to the Commission. The Commission also proposes several structural and linguistic changes to the Safe Harbors section to increase the Rule's clarity.

(1) Criteria for Approval of Self-Regulatory Guidelines (Paragraph (b))

Paragraph (b) of the Rule's safe harbor provisions set forth the criteria the Commission will use to review an application for safe harbor status. Among other things, safe harbor applicants must demonstrate that they have an effective mandatory mechanism for the independent assessment of their members' compliance. The Rule outlines possible, non-exclusive, methods applicants may employ to conduct this independent review,

¹⁷⁵ See 16 CFR 312.10(b)(1).

¹⁷⁶ See 16 CFR 312.10(b)(2)(i)–(iv).

¹⁷⁷ See 16 CFR 312.10(b)(3)(i)–(v). Effective incentives include mandatory public reporting of disciplinary action taken against participants by the safe harbor program; consumer redress; voluntary payments to the United States Treasury; referral of violators to the Commission; or any other equally effective incentive. *Id.*

¹⁷⁸ See TRUSTe (comment 64), at 6.

¹⁷⁹ See Harry A. Valetk (comment 66), at 4.

including periodic comprehensive or random checks of members' information practices, seeding members' databases if coupled with random or periodic checks,¹⁸⁰ or "any other equally effective independent assessment mechanism."¹⁸¹

The Commission proposes maintaining the standard that safe harbor programs implement "an effective, mandatory mechanism for the independent assessment of subject operators' compliance." Rather than provide a set of alternative mechanisms that safe harbor programs can use to carry out this requirement, the Commission proposes to mandate that, at a minimum, safe harbor programs conduct annual, comprehensive reviews of each of their members' information practices. In the Commission's view, this baseline benchmark for oversight will improve the accountability and transparency of Commission-approved COPPA safe harbor programs.

Therefore, the Commission proposes to amend paragraph (b)(2) of the safe harbor provisions of the Rule to read:

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(2) Request for Commission Approval of Self-Regulatory Program Guidelines (Paragraph (c))

Paragraph (c) of the Rule's current safe harbor provision sets forth the application requirements for safe harbor status. Among other things, an applicant must include the full text of the guidelines for which approval is sought and any accompanying commentary, a statement explaining how the applicant's proposed self-regulatory guidelines meet COPPA, and how the independent assessment mechanism and effective incentives for subject operators' compliance (required under paragraphs (b)(2) and (3)) provide effective enforcement of COPPA.¹⁸²

To enhance the reliability and sustainability of programs granted safe

harbor status,¹⁸³ the Commission proposes adding a requirement that program applicants include with their application a detailed explanation of their business model and the technological capabilities and mechanisms they will use for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program. This requirement will enable the Commission to better evaluate the qualifications of a safe harbor program applicant.

Therefore, the Commission proposes adding a new requirement to paragraph (c) (paragraph (c)(1)) that reads:

(c) *Request for Commission approval of self-regulatory program guidelines.* To obtain Commission approval of self-regulatory program guidelines, proposed safe harbor programs must file a request for such approval. A request shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program.¹⁸⁴

(3) Safe Harbor Reporting and Recordkeeping Requirements (Paragraph (d))

Paragraph (d) of the current safe harbor provision requires Commission-approved safe harbor programs to maintain records of consumer complaints, disciplinary actions, and the results of the independent assessments required under paragraph (b)(2) for a period of at least three years. Such records shall be made available to the Commission for inspection and copying at the Commission's request.¹⁸⁵

One commenter urged the Commission to make greater use of its inspection powers under paragraph (d) to audit safe harbor programs in order to "give the Commission a better understanding of actual marketplace practices, and inspire commercial operators to improve online practices."¹⁸⁶ The Institute for Public Representation went further, asking the Commission to "assess the effectiveness of the safe harbor programs by requiring annual reports about their enforcement efforts."¹⁸⁷ The Commission believes that instituting a periodic reporting requirement, in addition to retaining the

right to access program records, will better ensure that all safe harbor programs maintain sufficient records and that the Commission is routinely apprised of key information about approved safe harbor programs and their members. Therefore, the Commission proposes modifying paragraph (d) to require, within one year of the effective date of the Final Rule amendments, and every eighteen months thereafter, the submission of reports to the Commission containing, at a minimum, the results of an independent audit described in revised paragraph (b)(2), and the reporting of any disciplinary action taken against any member operator within the relevant reporting period.

Therefore, the Commission proposes modifying paragraph (d) to read:

(d) *Reporting and recordkeeping requirements.* Approved safe harbor programs shall:

(1) Within one year after the effective date of the Final Rule amendments, and every eighteen months thereafter, submit a report to the Commission containing, at a minimum, the results of the independent assessment conducted under paragraph (b)(2), a description of any disciplinary action taken against any subject operator under paragraph (b)(3), and a description of any approvals of member operators' use of parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to requests by the Commission for additional information; and,

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2).

(4) Revisions to Increase the Clarity of the Safe Harbor Provisions

The Commission also proposes a general reorganization of the safe harbor provision to provide a clearer roadmap of the requirements for obtaining and maintaining safe harbor status. This reorganization includes consolidating into separate paragraphs: the criteria for approval of self-regulatory program guidelines; the application requirements for Commission approval; reporting and recordkeeping requirements; post-approval modifications to self-regulatory program guidelines; and revocation of approval of self-regulatory program guidelines.¹⁸⁸ In addition, the

¹⁸⁸ The Commission also proposes deleting the requirement that the Commission must determine "in fact" that approved self-regulatory program guidelines or their implementation do not meet the

¹⁸⁰ "Seeding" a participant's database means registering as a child on the Web site or online service and then monitoring the site or service to ensure that it complies with the Rule's requirements.

¹⁸¹ See 16 CFR 312.10(b)(2).

¹⁸² See 16 CFR 312.10(c).

¹⁸³ See TRUSTe (comment 64), at 6.

¹⁸⁴ The Commission will consider applicants' requests that certain materials submitted in connection with an application for safe harbor should receive confidential treatment. See FTC Operating Manual, 15.5.1, and 15.5.2.

¹⁸⁵ See 16 CFR 312.10(d).

¹⁸⁶ See Harry A. Valetk (comment 66), at 4.

¹⁸⁷ See Institute for Public Representation (comment 33), at 37.

Commission proposes adding language to the revocation of approval paragraph to require currently approved safe harbor programs to propose modifications to their guidelines within 60 days of publication of the Final Rule amendments in order to come into compliance or face revocation.¹⁸⁹ Finally, the proposed revision would move to the end of this section the Rule's provision on the effect of an operators' participation in a safe harbor program.

VI. Request for Comment

The Commission invites interested persons to submit written comments on any issue of fact, law, or policy that may bear upon the proposals under consideration. Please include explanations for any answers provided, as well as supporting evidence where appropriate. After evaluating the comments, the Commission will determine whether to issue specific amendments.

Comments should refer to "COPPA Rule Review: FTC File No. P104503" to facilitate the organization of comments. Please note that your comment—including your name and your state—will be placed on the public record of this proceeding, including on the publicly accessible FTC Web site, at <http://www.ftc.gov/os/publiccomments.shtm>. Comments must be received on or before the deadline specified above in the **DATES** section in order to be considered by the Commission.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before November 28, 2011. Write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Web site, at <http://www.ftc.gov/os/publiccomments.shtm>. As a matter of discretion, the Commission tries to

requirements of the Rule's safe harbor provisions prior to revoking their approval.

¹⁸⁹ Therefore, the Commission proposes to amend paragraph (f) of the safe harbor provisions of the Rule to read:

(f) *Revocation of approval of self-regulatory program guidelines.* The Commission reserves the right to revoke any approval granted under this Section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, within 60 days of publication of the Final Rule amendments, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

remove individuals' home contact information from comments before placing them on the Commission Web site.

Because your comment will be made public, you are solely responsible for making sure that your comment doesn't include any sensitive personal information, such as anyone's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment doesn't include any sensitive health information, like medical records or other individually identifiable health information. In addition, don't include any "[t]rade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential," as provided in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). In particular, don't include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you must follow the procedure explained in FTC Rule 4.9(c), 16 CFR 4.9(c).¹⁹⁰ Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at <https://ftcpublic.commentworks.com/ftc/2011coppafulereview>, by following the instructions on the web-based form. If this document appears at <http://www.regulations.gov/#/home>, you also may file a comment through that Web site.

If you file your comment on paper, write "COPPA Rule Review, 16 CFR part 312, Project No. P104503" on your comment and on the envelope, and mail or deliver it to the following address: Federal Trade Commission, Office of the

¹⁹⁰ In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. See FTC Rule 4.9(c), 16 CFR 4.9(c).

Secretary, Room H-113 (Annex E), 600 Pennsylvania Avenue, NW., Washington, DC 20580. If possible, submit your paper comment to the Commission by courier or overnight service.

Visit the Commission Web site at <http://www.ftc.gov> to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before November 28, 2011.¹⁹¹ You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at <http://www.ftc.gov/ftc/privacy.htm>.

Comments on any proposed recordkeeping, disclosure, or reporting requirements subject to review under the Paperwork Reduction Act should additionally be submitted to OMB. If sent by U.S. mail, they should be addressed to Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission, New Executive Office Building, Docket Library, Room 10102, 725 17th Street, NW., Washington, DC 20503. Comments sent to OMB by U.S. postal mail, however, are subject to delays due to heightened security precautions. Thus, comments instead should be sent by facsimile to (202) 395-5167.

VII. Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980 ("RFA"), 5 U.S.C. 601 *et seq.*, requires a description and analysis of proposed and final rules that will have significant economic impact on a substantial number of small entities. The RFA requires an agency to provide an Initial Regulatory Flexibility Analysis ("IRFA") with the proposed Rule, and a Final Regulatory Flexibility Analysis ("FRFA"), if any, with the final Rule.¹⁹² The Commission is not required to make such analyses if a Rule would not have such an economic effect.¹⁹³

Although, as described below, the Commission does not anticipate that the proposed changes to the Rule will result in substantially more Web sites and online services being subject to the Rule, it will result in greater disclosure, reporting, and compliance

¹⁹¹ Questions for the public regarding proposed revisions to the Rule are found at Part X., *infra*.

¹⁹² See 5 U.S.C. 603-04.

¹⁹³ See 5 U.S.C. 605.

responsibilities for all entities covered by the Rule. The Commission believes that a number of operators of Web sites and online services potentially affected by the revisions are small entities as defined by the RFA. It is unclear whether the proposed amended Rule will have a significant economic impact on these small entities. Thus, to obtain more information about the impact of the proposed Rule on small entities, the Commission has decided to publish the following IRFA pursuant to the RFA and to request public comment on the impact on small businesses of its proposed amended Rule.

A. Description of the Reasons That Agency Action Is Being Considered

As described in Part I above, the Commission commenced a voluntary review of the COPPA Rule in early April 2010, seeking public comment on whether technological changes to the online environment warranted any changes to the Rule.¹⁹⁴ After careful review of the comments received, the Commission concludes that there is a need to update certain Rule provisions. Therefore, it proposes modifications to the Rule in the following five areas: Definitions, Notice, Parental Consent, Confidentiality and Security of Children's Personal Information, and Safe Harbor Programs. In addition, the Commission proposes adding a new Section to the Rule regarding data retention and deletion.

B. Succinct Statement of the Objectives of, and Legal Basis for, the Revised Proposed Rule

The objectives of the amendments are to update the Rule to ensure that children's online privacy continues to be protected, as directed by Congress, even as new online technologies evolve, and to clarify existing obligations for operators under the Rule. The legal basis for the proposed amendments is the Children's Online Privacy Protection Act, 15 U.S.C. 6501 *et seq.*

C. Description and Estimate of the Number of Small Entities to Which the Revised Proposed Rule Will Apply

The proposed amendments to the Rule will affect operators of Web sites and online services directed to children, as well as those operators that have actual knowledge that they are collecting personal information from children. The proposed Rule amendments will impose costs on entities that are "operators" under the Rule.

The Commission staff is unaware of any empirical evidence concerning the number of operators subject to the Rule. However, based on our compliance monitoring efforts in the area of children's privacy, data received by the Commission in connection with preparing its most recent studies of food marketing to children and marketing of violent entertainment to children, and the recent growth in interactive mobile applications that may be directed to children, the Commission staff estimates that approximately 2,000 operators may be subject to the Rule's requirements.

Under the Small Business Size Standards issued by the Small Business Administration, "Internet publishing and broadcasting and web search portals" qualify as small businesses if they have fewer than 500 employees.¹⁹⁵ The Commission staff estimates that approximately 80% of operators potentially subject to the Rule qualify as small entities. The Commission staff bases this estimate on its experience in this area, which includes its law enforcement activities, oversight of safe harbor programs, conducting relevant workshops, and discussions with industry and privacy professionals. The Commission seeks comment and information with regard to the estimated number or nature of small business entities on which the proposed Rule would have a significant economic impact.

D. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements

The proposed amended Rule would impose reporting, recordkeeping, and other compliance requirements within the meaning of the Paperwork Reduction Act, as set forth in Part VIII. of this Notice of Proposed Rulemaking. Therefore, the Commission is submitting the proposed requirements to OMB for review before issuing a final rule.

The proposed Rule likely would increase the recordkeeping, reporting, and other compliance requirements for covered operators. In particular, the proposed requirement that the direct notice to parents include more specific details about an operator's information collection practices, pursuant to a revised § 312.4 (Notice), would impose a one-time cost on operators. The Commission's proposed elimination of the sliding scale for acceptable mechanisms of obtaining parental

consent, pursuant to a revised § 312.5 (consent mechanisms for verifiable parental consent), would require those operators who previously used the e-mail plus method to now use a more reliable method for obtaining parental consent. The addition of proposed language in § 312.8 (confidentiality, security, and integrity of personal information collected from children) would require operators to take reasonable measures to ensure that service providers and third parties to whom they release children's personal information have in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information. Finally, the proposed Rule contains additional reporting requirements for entities voluntarily seeking approval to be a COPPA safe harbor self-regulatory program, and additional reporting and recordkeeping requirements for all Commission-approved safe harbor programs. Each of these proposed improvements to the Rule may entail some added cost burden to operators, including those that qualify as small entities.

The estimated burden imposed by these proposed amendments is discussed in the Paperwork Reduction Act section of this document, and there should be no difference in that burden as applied to small businesses. While the Rule's compliance obligations apply equally to all entities subject to the Rule, it is unclear whether the economic burden on small entities will be the same as or greater than the burden on other entities. That determination would depend upon a particular entity's compliance costs, some of which may be largely fixed for all entities (*e.g.*, Web site programming) and others variable (*e.g.*, Safe Harbor participation), and the entity's income or profit from operation of the Web site itself (*e.g.*, membership fees) or related sources (*e.g.*, revenue from marketing to children through the site). As explained in the Paperwork Reduction Act section, in order to comply with the rule's requirements, Web site operators will require the professional skills of legal (lawyers or similar professionals) and technical (*e.g.*, computer programmers) personnel. As explained earlier, the Commission staff estimates that there are approximately 2,000 Web site or online services that would qualify as operators under the proposed Rule, and that approximately 80% of such operators would qualify as small entities under the SBA's Small Business Size standards. The Commission invites

¹⁹⁴ See 75 FR 17089 (Apr. 5, 2010).

¹⁹⁵ See U.S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes, available at http://www.sba.gov/sites/default/files/Size_Standards_Table.pdf.

comment and information on these issues.

E. Identification of Other Duplicative, Overlapping, or Conflicting Federal Rules

The Commission has not identified any other federal statutes, rules, or policies that would duplicate, overlap, or conflict with the proposed Rule. The Commission invites comment and information on this issue.

F. Description of Any Significant Alternatives to the Proposed Rule

In drafting the proposed amended Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. The Commission believes that the proposed amendments are necessary in order to continue to protect children's online privacy in accordance with the purposes of COPPA. For each of the proposed amendments, the Commission has attempted to tailor the provision to any concerns evidenced by the record to date. On balance, the Commission believes that the benefits to children and their parents outweigh the costs of implementation to industry.

The Commission considered, but decided against, providing an exemption for small businesses. The primary purpose of COPPA is to protect children's online privacy by requiring verifiable parental consent before an operator collects personal information. The record and the Commission's enforcement experience have shown that the threats to children's privacy are just as great, if not greater, from small businesses or even individuals than from large businesses.¹⁹⁶ Accordingly, any exemption for small businesses would undermine the very purpose of the Statute and Rule.

Nonetheless, the Commission has taken care in developing the proposed amendments to set performance standards that will establish the objective results that must be achieved by regulated entities, but do not mandate a particular technology that must be employed in achieving these objectives. For example, the Commission has retained the standard that verifiable parental consent may be

obtained via a means reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The proposed new requirements for maintaining the security of children's personal information and deleting such information when no longer needed do not mandate any specific means to accomplish those objectives. The Commission also proposes to make it easier for operators to avoid the collection of children's personal information by adopting a "reasonable measures" standard enabling operators to use competent filtering technologies to prevent children's public disclosure of information.

The Commission seeks comments on ways in which the Rule could be modified to reduce any costs or burdens for small entities.

VIII. Paperwork Reduction Act

The existing Rule contains recordkeeping, disclosure, and reporting requirements that constitute "information collection requirements" as defined by 5 CFR 1320.3(c) under the OMB regulations that implement the Paperwork Reduction Act ("PRA"), 44 U.S.C. 3501 *et seq.* OMB has approved the Rule's existing information collection requirements through July 31, 2014 (OMB Control No. 3084-0117).

The proposed amendments to the COPPA Rule would change the definition of "personal information," potentially increasing the number of operators subject to the Rule. The proposed amendments also would eliminate e-mail plus as an acceptable method for obtaining parental consent, require operators to provide parents with a more detailed direct notice, and increase reporting and recordkeeping requirements for Commission-approved safe harbor programs. Accordingly, the Commission is providing PRA burden estimates for the proposed amendments, which are set forth below.

The Commission invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (2) the accuracy of the FTC's estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of collecting information on those who respond, including through the use of automated collection techniques or other forms of information technology.

Estimated Additional Annual Hours Burden

A. Number of Respondents

As noted in the Regulatory Flexibility Section of this NPR, Commission staff estimates that there are currently approximately 2,000 operators subject to the Rule. The Commission believes that the number of operators subject to the Rule's requirements will not change significantly as a result of the proposed revisions to the definition of personal information. Even though altering the definition of personal information potentially expands the pool of covered operators, other proposed changes in the Rule should offset much of this potential expansion. Specifically, these offsets include provisions allowing the use of persistent identifiers to support the internal operations of a Web site or online service, and permitting the use of reasonable measures such as automated filtering to strip out personal information before posting children's content in interactive venues. The Commission also anticipates many of these potentially new operators will make adjustments to their information collection practices so that they will not be collecting personal information from children, as defined by the Rule.

For this burden analysis, the Commission staff retains its recently published estimate of 100 new operators per year¹⁹⁷ for a prospective three-year PRA clearance period.¹⁹⁸ The Commission staff also retains its estimate that no more than one additional safe harbor applicant will submit a request within the next three years.

B. Recordkeeping Hours

The proposed Rule amendments do not impose any new significant recordkeeping requirements on operators. The proposed amendments do impose additional recordkeeping requirements on safe harbor programs, however. Commission staff estimates that in the year of implementation ("Year 1"), the four existing safe harbor programs will require no more than 100 hours to set up and implement a new recordkeeping system to comply with the proposed amendments.¹⁹⁹ In later

¹⁹⁶ See, e.g., *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal., filed Aug. 12, 2011); *United States v. Industrious Kid, Inc.*, No. CV-08-0639 (N.D. Cal., filed Jan. 28, 2008); *United States v. Xanga.com, Inc.*, No. 06-CIV-6853 (S.D.N.Y., filed Sept. 7, 2006); *United States v. Bonzi Software, Inc.*, No. CV-04-1048 (C.D. Cal., filed Feb. 17, 2004); *United States v. Looksmart, Ltd.*, Civil Action No. 01-605-A (E.D. Va., filed Apr. 18, 2001); *United States v. Bigmailbox.Com, Inc.*, Civil Action No. 01-606-B (E.D. Va., filed Apr. 18, 2001).

¹⁹⁷ See Agency Information Collection Activities; Submission for OMB Review; Comment Request; Extension, 76 FR 31334 (May 31, 2011) ("FTC COPPA PRA Extension").

¹⁹⁸ Under the PRA, agencies may seek a maximum of three years' clearance for a collection of information. 44 U.S.C. 3507(g). Recordkeeping, disclosure, and reporting requirements are all forms of information collection. See 44 U.S.C. 3502(3).

¹⁹⁹ See, e.g., Telemarketing Sales Rule ("TSR"), Notice of Proposed Rulemaking, 74 FR 41988,

years, once compliant systems are established, the burden for these entities should be negligible—no more than one hour each year.²⁰⁰ Thus, annualized burden per year for a prospective three-year clearance for existing safe harbor programs is 34 hours per safe harbor program (100 + 1 + 1 = 102 hours; 102 hours) 3 = 34 hour per year).

Accordingly, for the four existing safe harbor programs, cumulative annualized recordkeeping burden would be 136 hours.

For a new entrant, the initial burden of establishing recordkeeping systems and the burden of maintenance thereafter should be no more than for the existing safe harbors. Assuming, as noted above, that there will be one new safe harbor entrant per a given three-year PRA clearance period, the incremental annualized recordkeeping burden for the entrant under the proposed amendments would be 34 hours.

Thus, cumulative annualized recordkeeping burden for new and existing safe harbor applicants would be 170 hours.

C. Disclosure Hours

(1) New Operators' Disclosure Burden

Under the existing OMB clearance for the Rule, the Commission staff has already accounted for the time that new operators will spend to craft a privacy policy (approximately 60 hours per operator), design mechanisms to provide the required online privacy notice and, where applicable, direct notice to parents in order to obtain verifiable consent. The proposed amendments should no more than minimally add to, if at all, the time required to accomplish this task because their effect primarily is to transfer required information from the privacy policy to the direct notice.

(2) Existing Operators' Disclosure Burden

In Year 1, operators would have a one-time burden to re-design their existing privacy policies and direct notice procedures that would not carry over to the second and third years of prospective PRA clearance. In addition, existing operators that currently use the e-mail plus method would incur burden in Year 1 for converting to a more reliable method of parental verification. Commission staff believes that an existing operator's time to make these changes would be no more than that estimated for a new entrant to craft a

privacy policy for the first time, *i.e.*, 60 hours. Annualized over three years of PRA clearance, this amounts to 20 hours ((60 hours + 0 + 0) 3) per year. Aggregated for the 2,000 existing operators, annualized disclosure burden would be 40,000 hours.

D. Reporting Hours

The FTC previously has estimated that a prospective safe harbor organization requires 265 hours to prepare and submit its safe harbor proposal.²⁰¹ The proposed Rule amendments, however, require a safe harbor applicant to submit a more detailed proposal than what the current Rule mandates. Existing safe harbor programs will thus need to submit a revised application and new safe harbor applicants will have to provide greater detail than they would under the current Rule. The FTC estimates this added information would entail approximately 60 additional hours for safe harbors to prepare. Accordingly, the aggregate incremental burden for this added one-time preparation is 300 hours (60 hours × 5 safe harbors) or, annualized for an average single year per three-year PRA clearance, 100 hours.

The proposed amendments to the Rule require safe harbor programs to audit their members at least annually and to submit periodic reports to the Commission on the results of their audits of members. As such, this will increase currently cleared burden estimates pertaining to safe harbor applicants. The burden for conducting member audits and preparing these reports will likely vary for each safe harbor program depending on the number of members. The Commission staff estimates that conducting audits and preparing reports will require approximately 100 hours per program per year. Aggregated for five safe harbor programs, this amounts to an increased disclosure burden of 500 hours per year. Accordingly, cumulative yearly reporting burden for five safe harbor applicants to provide the added information proposed and to conduct audits and prepare reports is 600 hours.

E. Labor Costs

(1) Recordkeeping

Based on the above estimate of 170 hours for existing and new safe harbor programs, annualized for an average single year per three-year PRA

²⁰¹ For PRA purposes, annualized over the course of three years of clearance, this averages roughly 100 hours per year given that the 265 hours is a one-time, not recurring, expenditure of time for an applicant.

clearance, and applying a skilled labor rate of \$26/hour,²⁰² associated labor costs are \$4,420 per year.

(2) Disclosure

The Commission staff assumes that the time spent on compliance for operators would be apportioned five to one between legal (lawyers or similar professionals) and technical (*e.g.*, computer programmers) personnel.²⁰³ As noted above, the Commission staff estimates a total of 40,000 hours disclosure burden, annualized, for 2,000 existing operators. Thus, apportioned five to one, this amounts to, rounded, 33,333 hours of legal, and 6,667 hours of technical, assistance. Applying hourly rates of \$150 and \$36, respectively, for these personnel categories,²⁰⁴ associated labor costs would total approximately \$5,240,000.

(3) Reporting

The Commission staff assumes that the task to prepare safe harbor program applications will be performed primarily by lawyers at a mean labor rate of \$150 an hour. Thus, applied to an assumed industry total of 500 hours per year for this task, associated yearly labor costs would total \$75,000.

The Commission staff assumes periodic reports will be prepared by compliance officers, at a labor rate of \$28.²⁰⁵ Applied to an assumed industry total of 500 hours per year for this task, associated yearly labor costs would be \$14,000.

Cumulatively, labor costs for the above-noted reporting requirements total approximately \$89,000 per year.

F. Non-Labor/Capital Costs

Because both operators and safe harbor programs will already be equipped with the computer equipment and software necessary to comply with the Rule's notice requirements, the proposed amendments to the Rule

²⁰² This rounded figure is derived from the mean hourly earnings shown for computer support specialists found in the Bureau of Labor Statistics National Compensation Survey: Occupational Earnings in the United States, 2010, at Table 3, available at <http://www.bls.gov/ncs/ocs/sp/nctb1477.pdf> ("National Compensation Survey Table 3").

²⁰³ See FTC COPPA PRA Extension, 76 FR at 31335 n. 1.

²⁰⁴ The estimated rate of \$150 per hour is roughly midway between Bureau of Labor Statistics (BLS) mean hourly wages for lawyers (approximately \$54) in the most recent whole-year data (2010) available online and what Commission staff believes more generally reflects hourly attorney costs (\$250) associated with Commission information collection activities. The \$36 estimate of mean hourly wages for computer programmers also is based on the most recent whole-year BLS data. See National Compensation Survey Table 3.

²⁰⁵ See National Compensation Survey Table 3.

42013 (Aug. 19, 2009). Arguably, this estimate conservatively errs upward in the instant context.

²⁰⁰ *Id.*

should not impose any additional capital or other non-labor costs.

IX. Communications by Outside Parties to the Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding, from any outside party to any Commissioner or Commissioner's advisor, will be placed on the public record. See 16 CFR 1.26(b)(5).

X. Questions for the Proposed Revisions to the Rule

The Commission is seeking comment on various aspects of the proposed Rule, and is particularly interested in receiving comment on the questions that follow. These questions are designed to assist the public and should not be construed as a limitation on the issues on which public comment may be submitted. Responses to these questions should cite the numbers and subsection of the questions being answered. For all comments submitted, please submit any relevant data, statistics, or any other evidence, upon which those comments are based.

General Questions

1. Please provide comment on any or all of the provisions in the proposed Rule. For each provision commented on please describe (a) The impact of the provision(s) (including any benefits and costs), if any, and (b) what alternatives, if any, the Commission should consider, as well as the costs and benefits of those alternatives.

Definitions (§ 312.2)

2. Do the changes to the definition of "collects or collection" sufficiently encompass all the ways in which information can be collected online from children?

3. Does the "reasonable measures" standard articulated in the proposed definition of "collects or collection" adequately protect children while providing sufficient guidance to operators?

4. Are there identifiers that the Commission should consider adding to the list of "online contact information"?

5. Proposed § 312.2 would define personal information to include a "screen or user name."

a. What would be the impact of including "screen or user name" in the definition of personal information?

b. Is the limitation "used for functions other than or in addition to support for the internal operations of the Web site or online service" sufficiently clear to provide notice of the circumstances

under which screen or user name is covered by the Rule?

6. Proposed § 312.2 would define personal information to include a "persistent identifier."

a. What would be the impact of the changes to the term "persistent identifier" in the definition of personal information?

b. Is the limitation "used for functions other than or in addition to support for the internal operations of the Web site or online service" sufficiently clear to provide notice of the circumstances under which a persistent identifier is covered by the Rule?

c. Are there additional identifiers that the Commission should consider adding to the list of "persistent identifiers"?

7. Proposed § 312.2 would define personal information to include a "an identifier that links the activities of a child across different Web sites or online services." Is the language sufficiently clear to provide notice of the types of identifiers covered by this paragraph?

8. Proposed § 312.2 would define personal information to include "photograph, video, or audio file where such file contains a child's image or voice" and no longer requires that photographs (or similar items) be combined with "other information such that the combination permits physical or online contacting." What would be the impact of expanding the definition of personal information in this regard?

9. Are there identifiers that the Commission should consider adding to § 312.2's definition of "personal information"?

a. Should paragraph (e) of the definition of personal information include other forms of government-issued identification in addition to Social Security Number?

b. Does the combination of date of birth, gender, and ZIP code provide sufficient information to permit the contacting of a specific individual such that this combination of identifiers should be included as an item of personal information?

c. Should the Commission include "ZIP + 4" as an item of personal information?

10. Proposed § 312.2 would define "release of personal information" as "the sharing, selling, renting, or transfer of personal information to any third party." Is this definition sufficient to cover all potential secondary uses of children's personal information?

11. Proposed § 312.2 would define "support for the internal operations of the Web site or online service" as "those activities necessary to maintain the technical functioning of the Web site or

online service or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose."

a. Is the term "activities necessary to maintain the technical functioning" sufficiently clear to provide notice of the types of activities that constitute "support for the internal operations of the Web site or online service"? For example, is it sufficiently clear that the mere collection of an IP address, which is a necessary technical step in providing online content to web viewers, constitutes an "activity necessary to maintain the technical functioning of the Web site or online service"?

b. Should activities other than those necessary to maintain the technical functioning or to fulfill a request of a child under §§ 312.5(c)(3) and (4) be included within the definition of "support for the internal operations of the Web site or online service"?

Notice (§ 312.4)

12. Do the proposed changes to the "notice on the web site or online service" requirements in § 312.4(b) clarify or improve the quality of such notice?

13. Do the proposed changes to the "direct notice to the parent" requirements in § 312.4(c) clarify or improve the quality of such notices?

14. Should the Commission modify the notice requirement of the Rule to require that operators post a link to their online notice in any location where their mobile applications can be purchased or otherwise downloaded (e.g., in the descriptions of their applications in Apple's App Store or in Google's Android Market)?

15. Are there other effective ways of placing notices that should be included in the proposed revised Rule?

Parental Consent (§ 312.5)

16. Do the additional methods for parental consent set forth in proposed § 312.5(b)(2) sufficiently reflect available technologies to ensure that the person providing consent is the child's parent?

17. Should the Commission require operators to maintain records indicating that parental consent was obtained, and if so, what would constitute a sufficient record? What burdens would be imposed on operators by such a requirement?

18. Is there other information the Commission should take into account before declining to adopt certain parental consent mechanisms discussed

in Part V.C.(1). of the Notice of Proposed Rulemaking?

19. The Commission proposes eliminating the "email plus" mechanism of parental consent from § 312.5(b)(2). What are the costs and benefits to operators, parents, and children of eliminating this mechanism?

20. Proposed § 312.5(b)(3) would provide that operators subject to Commission-approved self-regulatory program guidelines may use a parental consent mechanism determined by such safe harbor program to meet the requirements of § 312.5(b)(1). Does proposed § 312.5(b)(3) provide a meaningful incentive for the development of new parental consent mechanisms? What are the potential downsides of this approach?

Confidentiality, Security and Integrity of Personal Information Collected From Children (§ 312.8)

21. Proposed § 312.8 would add the requirement that an operator "take reasonable measures to ensure that any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information."

a. What are the costs and benefits to operators, parents, and children of adding this requirement?

b. Does the language proposed by the Commission provide sufficient guidance and flexibility to operators to effectuate this requirement?

Data Retention and Deletion (§ 312.10)

22. The Commission proposes adding a requirement that an operator retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

a. Does the language proposed by the Commission provide sufficient guidance and flexibility to operators to effectuate this requirement?

b. Should the Commission propose specific time frames for data retention and deletion?

c. Should the Commission more specifically delineate what constitutes "reasonable measures to protect against unauthorized access to or use of the information"?

Safe Harbors (§ 312.11)

23. Proposed § 312.11(b)(2) would require safe harbor program applicants to conduct a comprehensive review of

all member operators' information policies, practices, and representations at least annually. Is this proposed annual review requirement reasonable? Would it go far enough to strengthen program oversight of member operators?

24. Proposed § 312.11(c)(1) would require safe harbor program applicants to include a detailed explanation of their business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of member operators' fitness for membership in the safe harbor program. Is this proposed requirement reasonable? Would it provide the Commission with useful information about an applicant's ability to run a safe harbor program?

25. Proposed § 312.11(d) would require Commission-approved safe harbor programs to submit periodic reports to the Commission regarding their oversight of member Web sites.

a. Should the Commission consider requiring safe harbor programs to submit reports on a more frequent basis, e.g., annually?

b. Should the Commission require that safe harbor programs report to the Commission a member's violations of program guidelines immediately upon their discovery by the safe harbor program?

Paperwork Reduction Act

26. The Commission solicits comments on whether the changes to the notice requirements (§ 312.4) and to the safe harbor requirements (§ 312.11), as well as the new data retention and deletion requirement (§ 312.10), constitute "collections of information" within the meaning of the Paperwork Reduction Act. The Commission requests comments that will enable it to:

a. Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

b. Evaluate the accuracy of the agency's estimate of the burden of the proposed collections of information, including the validity of the methodology and assumptions used;

c. Enhance the quality, utility, and clarity of the information to be collected; and,

d. Minimize the burden of the collections of information on those who must comply, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

XI. Proposed Revisions to the Rule

List of Subjects in 16 CFR Part 312

Children, Communications, Consumer protection, Electronic mail, E-mail, Internet, Online service, Privacy, Record retention, Safety, Science and Technology, Trade practices, Web site, Youth.

For the reasons discussed above, the Commission proposes to amend Part 312 of Title 16, Code of Federal Regulations, as follows:

PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE

1. The authority citation for part 312 continues to read as follows:

Authority: 15 U.S.C. 6501–6508.

2. Amend § 312.2 by revising the following definitions:

§ 312.2 Definitions.

* * * * *

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting, prompting, or encouraging a child to submit personal information online;

(b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or,

(c) Passive tracking of a child online.

* * * * *

Disclose or disclosure means, with respect to personal information:

(a) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and,

(b) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

* * * * *

Online contact information means an e-mail address or any other substantially similar identifier that permits direct

contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

* * * * *

Personal information means individually identifiable information about an individual collected online, including:

- (a) A first and last name;
- (b) A home or other physical address including street name and name of a city or town;
- (c) Online contact information as defined in this Section;
- (d) A screen or user name where such screen or user name is used for functions other than or in addition to support for the internal operations of the Web site or online service;
- (e) A telephone number;
- (f) A Social Security number;
- (g) A persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is used for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the Web site or online service;
- (h) An identifier that links the activities of a child across different Web sites or online services;
- (i) A photograph, video, or audio file where such file contains a child's image or voice;
- (j) Geolocation information sufficient to identify street name and name of a city or town; or,
- (k) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the Web site or online service means those activities necessary to maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose.

* * * * *

Web site or online service directed to children means a commercial Web site or online service, or portion thereof, that is targeted to children. Provided, however, that a commercial Web site or

online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial Web site or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In determining whether a commercial Web site or online service, or a portion thereof, is targeted to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

3. Amend § 312.4 by revising paragraphs (b) and (c) as follows:

§ 312.4 Notice.

* * * * *

(b) *Notice on the Web site or online service.* Pursuant to § 312.3(a), each operator of a Web site or online service directed to children must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and*, at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) Each operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and e-mail address;

(2) A description of what information each operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,

(3) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

(c) *Direct notice to a parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of the child's personal information, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(1) *Content of the direct notice to the parent required under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information.)* This direct notice shall set forth:

(i) That the operator has collected the parents' online contact information from the child in order to obtain the parent's consent;

(ii) That the parent's consent is required for the child's participation in the Web site or online service, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, if any, and the potential opportunities for the disclosure of personal information, if any, should the parent consent to the child's participation in the Web site or online service;

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b);

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and,

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) *Content of the direct notice to the parent allowed under § 312.5(c)(2) (Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information.)* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to the parent of a child's participation in a Web site or online service that does

not otherwise collect, use, or disclose children's personal information; and,

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the operator to allow the child to participate in the Web site or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and,

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(3) *Content of the direct notice to the parent required under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times.)* This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and,

(vi) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety.)* This direct notice shall set forth:

(i) That the operator has collected the child's name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and,

(v) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

4. Amend § 312.5 by revising paragraph (b)(2), by adding new paragraphs (b)(3) and (b)(4), and by revising paragraph (c), to read as follows:

§ 312.5 Parental consent.

* * * * *

(b) * * *

(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or an electronic scan; requiring a parent to use a credit card in connection with a monetary transaction; having a parent call a toll-free telephone number staffed by trained personnel; having a parent connect to trained personnel via video-conference; or, verifying a parent's identity by checking a form of government-issued identification against databases of such information, *provided that* the parent's identification is deleted by the operator from its records promptly after such verification is complete.

(3) *Commission approval of parental consent mechanisms.* Interested parties may file written requests for Commission approval of parental consent mechanisms not currently enumerated in paragraph (b)(2). To be considered for approval, parties must provide a detailed description of the proposed parental consent mechanism, together with an analysis of how the mechanism meets paragraph (b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 180 days of the filing of the request.

(4) *Safe harbor approval of parental consent mechanisms.* A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent mechanism not currently enumerated in paragraph (b)(2) where the safe harbor program determines that such parental consent mechanism meets the requirements of paragraph (b)(1).

(c) *Exceptions to prior parental consent.* Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in this paragraph:

(1) Where the sole purpose of collecting a parent's online contact information and the name of the child or the parent is to provide notice and obtain parental consent under

§ 312.4(c)(1) of this part. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the sole purpose of collecting a parent's online contact information is to provide notice to, and update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting a child's online contact information is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the sole purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(4). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the sole purpose of collecting a child's name, and a child's and a parent's online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the sole purpose of collecting a child's name and online contact information is to: (i) protect the security or integrity of its Web site or online service; (ii) take precautions against liability; (iii) respond to judicial process; or (iv) to the extent permitted under other provisions of law, to provide information to law enforcement

agencies or for an investigation on a matter related to public safety; and, where such information is not used for any other purpose.

5. Revise § 312.8 to read as follows:

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must take reasonable measures to ensure that any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

6. Revise § 312.10 to read as follows:

§ 312.10 Data retention and deletion requirements.

An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

7. Revise § 312.11 to read as follows:

§ 312.11 Safe harbor programs.

(a) *In general.* Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) *Criteria for approval of self-regulatory program guidelines.* Proposed safe harbor programs must demonstrate that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and § 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not

less than annually, of each subject operator's information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators' non-compliance with self-regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self-regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or,

(v) Any other equally effective action.

(c) *Request for Commission approval of self-regulatory program guidelines.* A proposed safe harbor program's request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program.

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and § 312.10 with the corresponding provisions of the guidelines; and,

(4) A statement explaining: (i) how the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and, (ii) how the assessment mechanisms and compliance consequences required under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) *Reporting and recordkeeping requirements.* Approved safe harbor programs shall:

(1) Within one year after the effective date of the Final Rule amendments, and every eighteen months thereafter, submit a report to the Commission containing, at a minimum, the results of the independent assessment conducted under paragraph (b)(2), a description of any disciplinary action taken against any subject operator under paragraph (b)(3), and a description of any approvals of member operators' use of

parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and,

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2).

(e) *Post-approval modifications to self-regulatory program guidelines.* Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2). The statement required under paragraph (c)(4) must describe how the proposed changes affect existing provisions of the guidelines.

(f) *Revocation of approval of self-regulatory program guidelines.* The Commission reserves the right to revoke any approval granted under this Section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, within 60 days of publication of the Final Rule amendments, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

(g) *Operators' participation in a safe harbor program.* An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and § 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 2011-24314 Filed 9-26-11; 8:45 am]

BILLING CODE 6750-01-P



Federal Trade Commission Protecting America's Consumers

For Your Information: 12/23/2011

FTC Seeks Public Comments on Facial Recognition Technology

Federal Trade Commission staff is seeking public comments on the issues raised at a recent FTC workshop exploring facial recognition technology and the privacy and security implications raised by its increasing use.

The December 8, 2011, public workshop, "Face Facts: A Forum on Facial Recognition Technology," focused on the current and future commercial applications of facial detection and recognition technologies, and explored an array of current uses of these technologies, possible future uses and benefits, and potential privacy and security concerns. The agenda for the workshop can be found [here](#), and an archived webcast of the proceedings is viewable [here](#). The deadline for filing comments is **January 31, 2012**, and instructions for filing can be found near the bottom of this press release.

Facial detection and recognition technologies have been adopted in a variety of new contexts, ranging from online social networks to digital signs and mobile apps. Their increased use has raised a variety of privacy concerns. To further the Commission's understanding of the issues, the Federal Trade Commission staff seeks public comments on issues raised at the workshop, including but not limited to:

- What are the current and future commercial uses of these technologies?
- How can consumers benefit from the use of these technologies?
- What are the privacy and security concerns surrounding the adoption of these technologies, and how do they vary depending on how the technologies are implemented?
- Are there special considerations that should be given for the use of these technologies on or by populations that may be particularly vulnerable, such as children?
- What are best practices for providing consumers with notice and choice regarding the use of these technologies?
- Are there situations where notice and choice are not necessary? By contrast, are there contexts or places where these technologies should not be deployed, even with notice and choice?
- Is notice and choice the best framework for dealing with the privacy concerns surrounding these technologies, or would other solutions be a better fit? If so, what are they?
- What are best practices for developing and deploying these technologies in a way that protects consumer privacy?

Public comments can be filed in electronic form by clicking [here](#) or in paper form by following the instructions located [here](#). Paper comments should refer to "Face Facts: A Forum on Facial Recognition -- Project Number P115406" and include this reference both in the text and on the envelope. They should be mailed or delivered to the Federal Trade Commission at the following address: 600 Pennsylvania Avenue N.W., Room H-113 (Annex P), Washington, DC 20580. Because all comments will be made publicly available on the FTC website, please do not include any trade secrets, confidential information, or sensitive personal information. The FTC is requesting that comments filed in paper form be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington, DC area and at the Commission is subject to delay due to heightened security precautions.

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's website provides free information on a variety of consumer topics. Like the FTC on Facebook and follow us on Twitter.

MEDIA CONTACT:

Office of Public Affairs
202-326-2180

STAFF CONTACT:

Amanda Koulousias

Division of Privacy and Identity Protection
202-326-3334

E-mail this News Release

If you send this link to someone else, the FTC will not collect any personal information about you or the recipient.

Related Items:

Last Modified: Friday, December 23, 2011

FTC Releases Proposed Revisions to Children's Online Privacy Protection Rule (COPPA)

September 16, 2011 | KELLEY DRYE CLIENT ADVISORY

On September 15, 2011, the Federal Trade Commission ("FTC") issued its [proposed amendments](#) to the Children's Online Privacy Protection Rule ("COPPA Rule" or the "Rule").¹ COPPA requires commercial websites and online services that target children to obtain verifiable parental consent before collecting personal information from children under the age of 13. The proposed revisions would modify or expand key definitions within the Rule, including the definition of "personal information," and would update the Rule's requirements concerning parental notice and consent, and existing safe harbor provisions. The proposed amendments also would include new safeguard requirements, including provisions that involve personal data minimization and disposal obligations.

The FTC's proposed revisions to the COPPA Rule are a response to the substantial changes in consumer technology that have occurred over the past decade since the Rule first became effective. Specifically, the proposed revisions are intended to ensure that the Rule continues to provide privacy protections for children who increasingly participate in social networking and interactive gaming, or engage in online activities through a mobile device. The FTC seeks written comments to the proposed amendments. Comments are due by November 28, 2011.

Proposed Revisions to the COPPA Rule

When The COPPA Rule Is Triggered

The COPPA Rule applies to both commercial websites and online services directed to children that collect personal information from a child. The Rule also applies to an online service that targets a general audience if that company has actual knowledge that it is collecting or maintaining personal information from a child.

While the Commission has advised that operators of general audience sites are not required to investigate the ages of their users, the Commission again emphasized in its commentary in the proposed amendments that if such companies ask for, or otherwise collect, information establishing that a user is under the age of 13, they will be subject to the COPPA Rule. This would include, for example, where an operator learns of a child's age or grade from the child's registration at the site, from a concerned parent who has learned that his child is participating at the site, and those that ask "age identifying" questions, such as "what type of school do you go to: (a) elementary; (b) middle; (c) high school; (d) college."

The FTC also clarified that, while it will not seek to expand COPPA to cover teenagers, it expects that companies will provide clear information to teenagers about the uses of their data and give them meaningful choices about such uses. Along those lines, the Commission is exploring new privacy approaches that will ensure that teens (and adults) benefit from stronger privacy protections than are currently generally available, including "just in time" privacy disclosures at the point when personal information is collected from the consumer. We expect to see more clarification on such a policy when the FTC Staff release the final *Privacy Report*, which will likely be issued later this year. The recommendations outlined in the Staff's draft *Privacy Report* are summarized in Kelley Drye's [December 8, 2010 client advisory](#).

Practice Areas

- Privacy and Information Security
- Advertising and Marketing
- FTC and State AG Investigations

Contacts

- Dana B. Rosenfeld
- John J. Heitmann
- Alysa Zeltzer Hutnik
- Christopher M. Loeffler
- Matthew P. Sullivan

Office

- Washington, D.C.

Finally, with respect to the Rule's application to "online services," the FTC stated that the Rule, as it currently stands, already covers the host of emerging technologies that connect online, including mobile applications that allow children to play network connected games, engage in social networking activities, purchase goods or services online, receive behaviorally targeted advertisements, or interact with other content or services, as well as Internet-enabled gaming platforms, voice-over-Internet protocol services, Internet-enabled location based services, some types of texting programs that connect online, including mobile applications that enable users to send text messages from their web-enabled devices without routing through a carrier-issued phone number constitute online services, and companies' premium texting and coupon texting programs that register users online and send text messages from the Internet to users' mobile phone numbers are online services. Thus, no changes were necessary to the Rule on this point.

Definitions

The FTC proposes revisions to a number of definitions within COPPA that are intended to either clarify current requirements or broaden the scope of defined terms to encompass technological developments that have occurred since the Rule was enacted. A brief description of the proposed changes is set forth below:

"Personal information": The most notable proposed changes to the definitions section is a significant expansion of the term "personal information" to include new forms of data that the FTC now considers personally identifiable. Under the proposed revisions, "personal information" would include online screen and user names, except in cases where such names are used solely for technical maintenance of the online service or website. "Personal information" also would include "online contact information" which includes identifiers that permit direct contact with a child online (including an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier. The revised definition also would cover photographs, and video or audio files containing a child's image or voice.

Notably, the FTC is proposing that "personal information" also include geolocation information emitted by a child's mobile or electronic device. This provision, if adopted, would expand the current location-based criteria under "personal information" that includes "a home or other physical address including street name and name of a city or town. The proposed revision responds to [recent concerns expressed by Congress and the FTC](#) over the extent to which mobile operators are collecting location information from user devices.

The Commission also proposes to broaden the meaning of the term "persistent identifier" as it applies to personal information. Under the current rule, a persistent identifier-including a website cookie, Internet Protocol ("IP") address, or a device serial number-must be linked to other information relating to a child or parent before it is classified as "personal information" under the rule. The FTC is proposing that a persistent identifier, standing alone, would be "personal information," unless the identifier is used solely to support the internal operations of the website or online service. The proposed revision would exempt a persistent identifier from the definition of personal information if it is used solely for user authentication, improving site navigation, serving contextual advertisements, or protecting against fraud or theft. Finally, a mobile device's unique identifier, or other identifier that can link a child's activities across different websites or online services also would fall within the "personal information" definition under the proposed changes.

"Collects or collection": The proposed revisions would update the definition of "collects or collection" to clarify that COPPA covers instances where an operator merely prompts or encourages a child to provide certain information, and not just when the operator mandates that information be provided to access the site. Further, the FTC is proposing language to clarify that "collects or collection" includes all forms of passive tracking of a child online, irrespective of the technology used.

The FTC also is proposing several modifications to the definition of "collects or collection" that it hopes will encourage operators to develop new processes that can delete virtually all personal information submitted by children before such information is made public. Specifically, the FTC would modify the current "100% deletion standard" that requires an operator to delete all individually identifiable information from its records and from postings by children before they're made public. In

its place, the Commission proposes a "reasonable measures" standard whereby operators who use technologies reasonably designed to capture all or virtually all personal information from children would not be deemed to have "collected" personal information.

"Release of personal information": The proposed rule revisions would clarify that "release of personal information" pertains to business-to-business uses of personal information, while "public disclosures of personal information" is addressed in COPPA's definition of "disclosure."

"Support for the internal operations of the website or online service": This term is used in the Rule to designate certain instances where a website operator may be permitted to use information provided by a child. The FTC's proposed changes would expand this definition to include "activities necessary to protect the security or integrity of the website or online service" in recognition of the website operators' need for protection from fraud and online security threats.

"Website or online service directed to children": Whether a website or online service is "directed to children" will continue to be based upon the totality of the circumstances. But as one of the factors that will be considered in evaluating whether the website is directed to children, the FTC proposes expanding the meaning of "audio content" to include music, and expressly noting that the use of a child celebrity on a website or online service is a strong indicator of the site's appeal to children.

Parental Notice

Streamlining Parental Notice. The COPPA Rule requires that a website or online service operator provide parents with two forms of notice concerning its intent to collect or use a child's information: (1) through the website or online service ("online notice"); and (2) through direct outreach to a parent whose child seeks to register on the site or service ("direct notice"). The Commission is proposing to streamline the current notice requirements in an effort to give parents easy-to-understand information provided on a real-time basis. This proposed revision is consistent with the FTC's previously noted preference that disclosure and notice information be "[embedded in the interaction](#)," as opposed to listed within lengthy privacy policies or terms of use.

Specifically, parents would receive notices through "just in time" messages that describe an operator's information practices at the most relevant points of interaction. The proposed revisions further describe the precise information that operators must provide to parents regarding: (1) the personal information that the operator has already obtained from the child; (2) the purpose of the notification; (3) actions that the parent must or may take; and (4) how the operator intends to use the personal information collected. For example, with respect to the notification purpose, the proposed revision would require that the operator's notice states that (1) the operator collected the parent's contact information in order to provide notice; (2) the parent's information will not be used for any other purpose; and (3) the parent may refuse to allow the child to participate in the site, and may require the deletion of his or her contact information. The FTC also would require that all forms of direct notice include a hyperlink to the operator's online notice of its information practices.

Notice Must Identify All Operators. The proposed revisions also would modify online notice requirements by mandating that *all* operators involved in the operation of an online service—and not just a designated operator, as permitted under the current Rule—provide contact information that includes the operator's name, physical address, telephone number, and email address. This revision specifically is intended to address the mobile applications environment in which multiple parties, including mobile app developers, advertising networks, and service providers are responsible for different functions in delivering the app to the consumer. The Commission believes this change will assist parents in finding the appropriate party to whom to direct an inquiry.

No Lengthy Policies for Parental Notice. The FTC's final proposed revision to the Notice section would eliminate the use of lengthy privacy policies to provide online notice and, instead, would require a simple statement that describes: (1) the information that the operator collects from children, and whether the child can make information publicly-available on the operator's site; (2) how the operator uses the child's information; and (3) the operator's disclosure practices for such information. The intent of the proposed change is to provide consumers with more readily-available and easy-to-understand information, given that an increasing amount of online content is provided over mobile

devices with smaller screen sizes.

Parental Consent Mechanisms

Expand Types of Parental Consent. The Commission is proposing several substantial changes to the mechanisms that an operator can use to obtain verifiable parental consent before it can collect, use, or disclose information obtained from children. For example, the proposed revisions would expand the methods by which operators can seek and obtain verifiable parental consent to include electronically-scanned versions of signed parental consent forms, videoconferencing, and government-issued identification - such as a driver's license - that is checked against a database. Operators could use such information for verification purposes only.

Payment Card Consent Only For Transactions. The Rule also would clarify that credit card information can be used for verification purposes only in instances where the parental consent is needed to facilitate an actual monetary transaction.

Eliminating Email Plus Verification. The FTC also has proposed eliminating the "email plus" method of verification now used by operators that collect children's personal information for internal use only. The method requires operators to obtain consent through an email to the parent, in concert with a separate verification step such as confirming the parent's consent by letter or telephone. The Commission, in an effort to strengthen verifiable consent procedures by leveraging new technologies, has proposed a new process through which operators may voluntarily seek Commission approval of potential consent mechanisms. Applicants seeking approval would be required to submit to the FTC a description of the mechanism, along with an analysis of how it complies with COPPA. The mechanism then would be subject to public comment before the Commission would grant approval.

Safe Harbor Parental Consent Okay. The FTC also has proposed adding a provision to the rule stating that operators participating in an FTC-approved safe harbor program may use any parental consent mechanisms deemed by the safe harbor program to meet COPPA requirements.

Confidentiality and Security of Children's Personal Information

Security Safeguards Required with Third Parties. COPPA requires operators to establish reasonable procedures to protect the confidentiality, integrity, and security of children's personal information; however, the current rule is silent on the data security obligations of third parties. The proposed revisions would add a requirement that operators take "reasonable measures" to ensure that any service provider or third party to whom children's personal information is provided has enacted "reasonable procedures" to protect the confidentiality, security, and integrity of such personal information.

Data Minimization Requirements. The proposed revisions also would impose a new data retention and deletion requirement, whereby operators could retain children's personal information only for so long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator also would be required to take reasonable measures to protect against unauthorized access to the information during the data deletion or disposal process.

The Role of Self-Regulation Programs

COPPA permits operators to participate in safe harbor programs that have created guidelines that protect children's online privacy to the same or greater extent as COPPA, and include processes to ensure that member participants comply with program's provisions. The FTC has proposed several modifications to the manner in which it oversees safe harbor programs:

Annual Audits of Program Members: Under the current rule, safe harbor programs are required only to conduct "periodic reviews" that may be conducted "on a random basis" to assess an operator's compliance with the program. The proposed revision would mandate that, at a minimum, safe harbor programs conduct annual, comprehensive reviews of each of their members' information practices as a way to improve accountability and transparency of such programs.

Provide FTC with Detailed Capabilities Overview. The Commission proposes adding a new

requirement that program applicants include with their safe harbor application a detailed explanation of their business model and the technological capabilities and mechanisms they will use to assess an operators' fitness for membership in the safe harbor program.

Report Periodically to the Commission: The Commission proposes modifying the current requirement that safe harbor programs maintain records of consumer complaints, disciplinary actions, and the results of independent assessments for 3 years, which must be made available to the Commission *upon request*. Under the proposed revision, safe harbor programs would be *required* to submit reports to the Commission that include the results of its independent audits, and reports on any disciplinary actions taken against members during the relevant reporting period. The reports would be due to the Commission within one year from the effective date of the final amendment, and every eighteen months thereafter.

Conclusion

During the past year, the Commission has been a vocal advocate for children's online privacy protections in response to continuing changes in the manner by which children view and interact with online content. The FTC [recently used its enforcement powers](#) to send a clear signal to website and mobile operators that target children, and the Commission is now employing its rulemaking authority to enhance current privacy protections for children. The FTC's proposed amendments to COPPA would impose significant new requirements on operators relating to parental notice and consent, the types of information that an operator can collect from children, and how such information must be protected. Because the FTC is able to levy fines of up to \$16,000 per violation for non-compliance with the COPPA Rule, these proposed changes come with teeth if the proposed changes are implemented, and companies fail to comply with them.

During this review period for the proposed changes, the FTC has invited the public to submit comments on any or all issues raised within its notice of proposed rulemaking ("NPRM"), as well as responses to specific questions listed in Section X of the NPRM. The filing deadline for comments is November 28, 2011. Please contact us, if we can be of assistance in the preparation of comments on your behalf.

Kelley Drye & Warren LLP

Kelley Drye & Warren's [Privacy and Information Security](#) practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

For more information about this advisory, contact:

[Dana B. Rosenfeld](#)
(202) 342-8588
drosenfeld@kelleydrye.com

[John J. Heitmann](#)
(202) 342-8544
jheitmann@kelleydrye.com

[Alysa Zeltzer Hutnik](#)
(202) 342-8603
ahutnik@kelleydrye.com

[Christopher M. Loeffler](#)

(202) 342-8429
cloeffler@kelleydrye.com

Matthew P. Sullivan
(202) 342-8869
msullivan@kelleydrye.com

¹ 16 C.F.R. Part 312.

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

**“AN EXAMINATION OF CHILDREN’S PRIVACY: NEW TECHNOLOGY
AND THE CHILDREN’S ONLINE PRIVACY PROTECTION ACT”**

**SUBCOMMITTEE ON CONSUMER PROTECTION,
PRODUCT SAFETY, AND INSURANCE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE**

Washington, DC

April 29, 2010

I. Introduction

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, my name is Jessica Rich, and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission (“Commission”).¹ I appreciate the opportunity to appear before you today to discuss the Commission’s implementation of the Children’s Online Privacy Protection Act of 1998 (“COPPA”).²

The Federal Trade Commission is deeply committed to helping to create a safer, more secure, online experience for children. As such, the agency has actively engaged in law enforcement, consumer and business education, and rulemaking initiatives to ensure that knowledge of, and adherence to, COPPA is widespread. In the past ten years, the Commission has brought fourteen law enforcement actions alleging COPPA violations and has collected more than \$3.2 million in civil penalties. In addition, in light of significant changes to the online environment, including the explosion of social networking and the proliferation of mobile web technologies and interactive gaming, and the possibility of interactive television, the Commission has recently initiated an accelerated review of COPPA’s effectiveness.

This testimony first provides a brief legislative and regulatory overview of COPPA. It next summarizes the Commission’s efforts to enforce COPPA and to educate businesses and consumers about the law. Finally, it discusses the Commission’s current initiative to review its

¹ While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

² See Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6508 (2009). The Commission’s implementing regulations (the “COPPA Rule”) are found at 16 C.F.R. Part 312 (2009).

COPPA Rule in order to determine whether the Rule should be modified to address changes in technology that may affect children’s privacy.

II. A Brief COPPA Overview

A. The Legislation

Congress enacted COPPA in 1998 to address the unique privacy and safety risks created when young children – those under 13 years of age – access the Internet. COPPA’s legislative history reveals several critical goals: (1) to enhance parental involvement in children’s online activities in order to protect children’s privacy; (2) to protect children’s safety when they visit and post information on public chat rooms and message boards; (3) to maintain the security of children’s personal information collected online; and (4) to limit the collection of personal information from children without parental consent.³

COPPA applies to operators of websites and online services directed to children under age 13, and to other website operators that have actual knowledge that they are collecting personal information⁴ from such children (collectively, “operators”). The statute generally mandates that operators covered by the Act provide notice of their information collection practices and, with only limited exceptions, obtain verifiable parental consent *prior* to the collection, use, or disclosure of personal information from children. Operators also must give

³ See 144 Cong. Rec. S12741 (Oct. 7, 1998) (statement of Sen. Bryan).

⁴ COPPA defines personal information as individually identifiable information about an individual collected online, including: a first and last name; a home or other physical address including street name and a name of a city or town; an e-mail address; a telephone number; a Social Security number; any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph. 15 U.S.C. § 6501(8).

parents the opportunity to review and delete personal information their children have provided. Operators are required to establish and maintain reasonable procedures to protect the security of personal information collected from children, and must not condition children's participation in website activities on the disclosure of more personal information than is reasonably necessary.⁵

COPPA contains a safe harbor provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines to implement the statute's protections.⁶ The statute provides that operators who fully comply with an approved safe harbor program will be "deemed to be in compliance" with the Commission's COPPA Rule for purposes of enforcement.⁷

B. The Commission's COPPA Rule

COPPA mandated that the Commission promulgate and enforce regulations to implement the Act. The Commission published for public comment a proposed Rule in April 1999, and in November 1999 published its final Rule, which went into effect on April 21, 2000.⁸

The Rule closely follows the statutory language, requiring operators to provide notice of their information practices to parents and, with limited exceptions, to obtain "verifiable parental consent" prior to collecting, using, or disclosing personal information from children under the

⁵ 15 U.S.C. § 6503(b)(1).

⁶ 15 U.S.C. § 6504. Since the Commission's COPPA Rule took effect on April 21, 2000, four groups have received Commission approval of their safe harbor programs: the Children's Advertising Review Unit of the National Advertising Division of the Council of Better Business Bureaus ("CARU"), the Entertainment Software Rating Board ("ESRB"), TRUSTe, and Privo, Inc. For information on the Commission's COPPA safe harbor process, *see* http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.

⁷ 15 U.S.C. § 6504(b)(2).

⁸ 16 C.F.R. § 312 (2009).

age of 13. Verifiable parental consent, as set forth in the Rule, means that operators must use a consent method that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.⁹ The COPPA Rule sets forth a sliding scale approach to obtaining verifiable parental consent based upon the risks posed by the intended uses of the child's information.¹⁰ Under this approach, operators who keep children's information internal, and do not disclose it publicly or to third parties, may obtain parental consent by methods such as sending an email to the parent and then following up to confirm consent.¹¹ By contrast, operators who disclose children's personal information to others must use a more reliable method of parental consent – either one of the methods outlined by the Commission, or an equivalent method designed to ensure that the operator is connecting with the child's parent.¹²

COPPA authorizes the Commission to enforce the Rule in the same manner as it does rules promulgated under Section 18(a)(1)(B) of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices.¹³ This permits the Commission to obtain civil penalties

⁹ 16 C.F.R. § 312.5(b)(1).

¹⁰ 16 C.F.R. § 312.5(b)(2).

¹¹ The sliding scale mechanism, which initially was designed to expire in April 2002, was subsequently extended by the Commission. In 2006, the Commission announced that it would extend the sliding scale approach indefinitely. *See* 71 Fed. Reg. 13247 (Mar. 15, 2006), available at www.ftc.gov/os/2006/03/P054505COPPARuleRetention.pdf.

¹² Such methods include, but are not limited to: using a print-and-send form that can be faxed or mailed back to the operator; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using email accompanied by a PIN or password obtained through one of the above methods. 16 C.F.R. § 312.5(b)(2).

¹³ 15 U.S.C. §§ 6503(c), 6506(a), (d); 15 U.S.C. § 57a(a)(1)(B) (2009).

against operators who violate the Rule. COPPA further authorizes state attorneys general to enforce compliance with the Rule by filing actions in federal court with written notice to the Commission.¹⁴

III. The Commission’s COPPA Enforcement and Education Efforts

A. Enforcing COPPA

In the ten years since the Rule’s enactment, the Commission has brought fourteen (14) COPPA enforcement actions that cut to the core of COPPA’s goals – ensuring that parents are informed and have the right to say “no” before their young children divulge their personal information. These rights are especially important when, with the mere click of a mouse or the touch of a screen, a child’s personal information can be viewed by anyone. Together, the Commission’s actions have garnered more than \$3.2 million dollars in civil penalties.¹⁵

In 2006, as social networking exploded onto the youth scene, the Commission redoubled its efforts to enforce COPPA. That year, the Commission obtained an order against Xanga.com, a then-popular social blogging site alleged to have knowingly collected personal information from, and created blog pages for, 1.7 million underage users – without obtaining their parents’ permission. The Xanga.com settlement included a \$1 million civil penalty.¹⁶

¹⁴ 15 U.S.C. § 6505. To date, only the state of Texas has filed law enforcement actions under the COPPA statute. *See* News Release, Office of Texas Attorney General Abbott Takes Action Against Web Sites That Illegally Collect Personal Information from Minors: Millions of Children Registered With The Popular Sites; Texas first state to take action under COPPA (Dec. 5, 2007), <http://www.oag.state.tx.us/oagNews/release.php?id=2288>.

¹⁵ News releases detailing each of the Commission’s COPPA cases are available at www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

¹⁶ *United States v. Xanga.com, Inc.*, No. 06-CIV-6853(SHS) (S.D.N.Y.) (final order Sept. 11, 2006).

In 2008, the Commission obtained orders against two other operators of social networking sites. In January of that year, operators of the child-directed social networking site, Imbee.com, paid \$130,000 to settle charges that they allegedly violated COPPA by collecting and maintaining personal information from over 10,500 children without first obtaining parental consent.¹⁷ Later that year, Sony BMG Music Entertainment paid a \$1 million civil penalty to resolve allegations that the company knowingly and improperly collected a broad range of personal information from at least 30,000 underage children who registered on 196 of its general audience music fan sites.¹⁸

Most recently, the Commission charged Iconix Brand Group, Inc., the owner and marketer of several apparel brands popular with children and teens, with collecting and storing personal information from approximately 1,000 children without first notifying their parents or obtaining parental consent. The Commission's complaint further alleged that on one of its brand websites, Iconix enabled girls to share personal stories and photos publicly online. Iconix agreed to pay a \$250,000 civil penalty to settle the Commission's charges.¹⁹

B. Consumer and Business Education

Although law enforcement is a critical part of the Commission's COPPA program, enforcement alone cannot accomplish all of the agency's goals in administering COPPA and the Rule. A crucial complement to the Commission's formal law enforcement efforts, therefore, is

¹⁷ *United States v. Industrious Kid, Inc.*, No. 08-CV-0639 (N.D. Cal.) (filed Jan. 29, 2008).

¹⁸ *United States v. Sony BMG Music Entm't*, No. 08-CV-10730 (S.D.N.Y.) (final order Dec. 15, 2008).

¹⁹ *United States v. Iconix Brand Group, Inc.*, No. 09-CV-8864 (S.D.N.Y.) (final order Nov. 5, 2009).

educating consumers and businesses about their rights and responsibilities under the law. By promoting business and consumer education, the Commission seeks to help the greater online community create a culture that protects children’s privacy and security.

The Commission’s business outreach goals focus broadly on shaping prospective practices. The agency devotes significant resources to assisting website operators with Rule compliance, regularly updating business education materials and responding to inquiries from operators and their counsel.²⁰

The Commission’s consumer education materials aim to inform parents and children about the protections afforded by the Rule and also provide them with general online privacy and safety information. The Commission’s consumer online safety portal, OnGuardOnline.gov, provides practical and plain language information in a variety of formats – including articles, games, quizzes, and videos – to help computer users guard against Internet fraud, secure their computers, and protect their personal information.²¹ The Commission’s booklet, *Net Cetera: Chatting With Kids About Being Online*, is a recent addition to OnGuardOnline.gov. This guide

²⁰ To facilitate COPPA compliance, the Commission maintains a comprehensive children’s privacy area on its website where businesses can find useful publications, including *How to Comply with the Children’s Online Privacy Protection Rule; You, Your Privacy Policy and COPPA*; and *How to Protect Kids’ Privacy Online*, as well as answers to Frequently Asked Questions (or “FAQs”). See <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html>. Periodically, the Commission issues guidance on specific topics, like the Rule’s requirements for the content of online privacy notices, and the COPPA “actual knowledge” standard for operators of general audience websites. In addition, the agency maintains a COPPA Hotline, where staff members offer fact-specific guidance in response to questions from website operators.

²¹ The OnGuardOnline.gov website is the central component of the OnGuardOnline consumer education campaign, a partnership of the federal government and the technology community. Currently, 13 federal agencies and a large number of safety organizations are partners on the website, contributing content and helping to promote and disseminate consistent messages.

gives practical tips on how parents, teachers, and other trusted adults can help children reduce the risks of inappropriate conduct, contact, and content that come with living life online. *Net Cetera* focuses on the importance of communicating with children about issues ranging from cyberbullying to sexting, social networking, mobile phone use, and online privacy.²² The Commission has partnered with schools, community groups, and local law enforcement to publicize *Net Cetera*, and has distributed more than 2.5 million copies of the guide since it was introduced in October 2009.

IV. The Current Regulatory Review

In 2005, the Commission commenced a statutorily required review of its experience in enforcing COPPA.²³ Specifically, Congress directed the Commission to evaluate: (1) operators' practices as they relate to the collection, use, and disclosure of children's information, (2) children's ability to obtain access to the online information of their choice; and (3) the availability of websites directed to children. At the same time, the Commission sought public comment on the costs and benefits of the Rule, including whether any modifications to the Rule were needed in light of changes in technology or in the marketplace.

After completing that review, in 2007 the Commission reported to Congress that, in keeping with the legislative intent, the Rule: (1) played a role in improving operators' information collection practices and providing children with greater online protections than in the era prior to its implementation; (2) provided parents with a set of effective tools for becoming involved in and overseeing their children's interactions online; and (3) did not overly

²² See OnGuardOnline, "Net Cetera: Chatting With Kids About Being Online," available at <http://www.onguardonline.gov/pdf/tec04.pdf>.

²³ See 15 U.S.C. § 6506(1).

burden operators' abilities to provide interactive online content for children. Accordingly, the Commission concluded that there was a continuing need for those protections, and that the Rule should be retained without change.²⁴ At that time, the Commission also acknowledged that children's growing embrace of mobile Internet technology and interactive general audience sites, including social networking sites, without the concomitant development of suitable age-verification technologies, presented challenges for COPPA compliance and enforcement.²⁵

Although the Commission generally reviews its rules approximately every ten years, the continued rapid-fire pace of technological change, including an explosion in children's use of mobile devices and participation in interactive gaming, and the possibility of interactive television, led the agency to accelerate its COPPA review by five years, to this year.²⁶

Accordingly, on March 24, 2010, the Commission announced the start of a public comment period aimed at gathering input on a wide range of issues relating to the COPPA Rule, including:

- The implications for COPPA enforcement raised by mobile communications, interactive television, interactive gaming, and other similar interactive media and whether the Rule's definition of "Internet" adequately encompasses these technologies;

²⁴ See Fed. Trade Comm'n, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* (2007), available at http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

²⁵ See *id.* at 28-29.

²⁶ The Commission recently concluded a series of privacy roundtables exploring the challenges posed by the array of new technologies that collect and use consumer data. The Commission also sought public comment on these issues and currently is examining the comments and information developed at the roundtables. In addition, the Commission expects that information gathered during the course of the COPPA Rule review will help inform this broader privacy initiative. See *Exploring Privacy: A Roundtable Series*, <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>.

- Whether operators have the ability, using persistent IP addresses, mobile geolocation data, or information collected from children online in connection with behavioral advertising, to contact specific individuals, and whether the Rule’s definition of “personal information” should be expanded accordingly;
- How the use of centralized authentication methods (such as OpenId) will affect individual websites’ COPPA compliance efforts;²⁷
- Whether there are additional technological methods to obtain verifiable parental consent that should be added to the COPPA Rule, and whether any of the methods currently included should be removed; and
- Whether parents are exercising their rights under the Rule to review or delete personal information collected from their children, and what challenges operators face in authenticating parents.²⁸

The period for comment on these questions will close on June 30, 2010. On June 2, before the comment period closes, the Commission will host a public roundtable at its Washington, DC Conference Center to hear from stakeholders – children’s privacy advocates,

²⁷ Centralized authentication methods offer a means for users to log on to different services using one digital identity. Services such as OpenId replace the common login process on individual websites with a single authenticated identification to gain access to multiple software systems. As a result, children who obtain an OpenId authentication might be able to gain back-door access to websites that otherwise would have provided them with COPPA protections or prevented their entry.

²⁸ See Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule, 75 Fed. Reg. 17089-93 (Apr. 5, 2010); see also News Release, Fed. Trade Comm’n, “FTC Seeks Comment on Children’s Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule” (Mar. 24, 2010), <http://www.ftc.gov/opa/2010/03/coppa.shtm>.

website operators, businesses, academics, and educators and parents – on these important issues.²⁹

V. Conclusion

The Commission takes seriously the challenge to ensure that COPPA continues to meet its originally stated goals, even as children’s interactive media use moves from stand-alone PCs, to handheld devices, and potentially beyond.

Thank you for this opportunity to discuss the Commission’s COPPA program. I look forward to your questions.

²⁹ See News Release, Fed. Trade Comm’n, “Protecting Kids’ Privacy Online: Reviewing the COPPA Rule” (Apr. 19, 2010), <http://www.ftc.gov/opa/2010/04/coppa.shtm>.

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

“PROTECTING YOUTHS IN AN ONLINE WORLD”

**SUBCOMMITTEE ON CONSUMER PROTECTION,
PRODUCT SAFETY, AND INSURANCE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE**

Washington, DC

July 15, 2010

I. INTRODUCTION

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, my name is Jessica Rich and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate this opportunity to appear before you today to discuss the Commission’s efforts to protect the privacy and security of teens in the digital environment.

The Federal Trade Commission is committed to protecting teens as they navigate digital technologies and applications. The agency has actively engaged in education, law enforcement, and policy efforts to help make the digital world safer for all consumers, including teens.

This testimony first highlights some of the privacy and safety risks teens face as they participate in the digital world. Second, it summarizes the Commission’s efforts to educate teens and their parents about these risks. Third, it highlights the Commission’s efforts to protect privacy in the context of technologies used heavily by teens in particular – social networking, mobile computing, and peer-to-peer (“P2P”) file-sharing programs. Finally, the testimony addresses proposals to create separate privacy protections for teens online.

II. TEENS IN THE DIGITAL ENVIRONMENT

Teens are heavy users of digital technology and new media applications including social networking, mobile devices, instant messaging, and file-sharing. Indeed, a 2007 study found

¹ While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

that over 90 percent of kids between the ages of 12 and 17 spend time online.² The online world has changed how teens learn, socialize, and are entertained. In many ways, the experiences teens have online are positive – they use the Internet to socialize with their peers,³ to learn more about topics that interest them,⁴ and to express themselves.⁵

But teens also face unique challenges online. For example, research shows that teens tend to be more impulsive than adults and that they may not think as clearly as adults about the consequences of what they do.⁶ As a result, they may voluntarily disclose more information online than they should. On social networking sites, young people may share personal details that leave them vulnerable to identity theft.⁷ They may also share details that could adversely

² Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, & Aaron Smith, Pew Internet & American Life Project, *Teens and Social Media* (Dec. 19, 2007), available at www.pewinternet.org/~media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.

³ See Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, *Social Networking Websites and Teens* (Jan. 2007), available at www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/More-details-from-the-survey.aspx?r=1.

⁴ See Kaiser Family Foundation, *Generation M2: Media in the Lives of 8- to 18-Year-Olds* (Jan. 2010), available at www.kff.org/entmedia/upload/8010.pdf.

⁵ See Amanda Lenhart, Kristen Purcell, Aaron Smith, & Kathryn Zickuhr, Pew Internet & American Life Project, *Social Media and Young Adults* (Feb. 2010), available at www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1.

⁶ See, e.g., Transcript of Exploring Privacy, A Roundtable Series (Mar. 17, 2010), Panel 3: Addressing Sensitive Information, available at htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/031710_sess3.pdf; Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (April 14, 2010), available at ssrn.com/abstract=1589864.

⁷ See Javelin Strategy and Research, *2010 Identity Fraud Survey Report* (Feb. 2010), available at www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf.

affect their potential employment or college admissions.⁸ Teens also sometimes “sex” to their peers – send text messages and images with sexual content – without considering the potential legal consequences and harm to their reputations. According to one recent study, 4 percent of cell phone owners aged 12 to 17 have sent sexually suggestive images of themselves by phone, while 15 percent have received “sexts” containing images of someone they know.⁹ In addition, bullies or predators – most often teens’ own peers – may try to take advantage of adolescents on the Internet. About one-third of all teens online have reported experiencing some kind of online harassment, including cyberbullying.¹⁰

Despite teens’ sharing and use of personal information in the digital world, there is data that suggests teens are concerned about their online privacy. For example, one study of teens and privacy found that teens engage in a variety of techniques to obscure or conceal their real location or personal details on social networking sites.¹¹ The Commission seeks to address these privacy concerns – as well as parents’ concerns about their teens’ online behavior and

⁸ See e.g., Commonsense Media, *Is Social Networking Changing Childhood? A National Poll* (Aug. 10, 2009), available at www.commonensemedia.org/sites/default/files/CSM_teen_social_media_080609_FINAL.pdf (indicating that 28 percent of teens have shared personal information online that they would not normally share publicly) .

⁹ Press Release, Pew Internet & American Life Project, *Teens and Sexting* (Dec. 15, 2009), available at www.pewinternet.org/Press-Releases/2009/Teens-and-Sexting.aspx.

¹⁰ Amanda Lenhart, Pew Internet & American Life Project, *Cyberbullying and Online Teens* (June 27, 2007), available at www.pewinternet.org/~media/Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf.

¹¹ Amanda Lenhart and Mary Madden, Pew Internet & American Life Project, *Teens, Privacy, and Online Social Networks* (Apr. 18, 2007), available at www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1.

interactions – through education, policy development, and law enforcement, as discussed further below.

III. CONSUMER EDUCATION

The FTC has launched a number of education initiatives designed to encourage consumers of all ages to use the Internet safely and responsibly. The Commission’s online safety portal, OnGuardOnline.gov, developed in partnership with other federal agencies, provides practical information in a variety of formats – including articles, game, quizzes, and videos – to help people guard against Internet fraud, secure their computers, and protect their personal information.¹² The Commission’s booklet, *Net Cetera: Chatting With Kids About Being Online*,¹³ is the most recent addition to the OnGuardOnline.gov consumer education campaign. This guide provides practical tips on how parents, teachers, and other trusted adults can help children of all ages, including teens and pre-teens, reduce the risks of inappropriate conduct, contact, and content that come with living life online.

Net Cetera focuses on the importance of communicating with children about issues ranging from cyberbullying to sexting, social networking, mobile phone use, and online privacy. It provides specific advice to parents about talking to their children about each of these topics. For example, on the subject of sexting, it discusses the risks sexting poses to kids’ reputations

¹² The OnGuardOnline.gov website is the central component of the OnGuardOnline consumer education campaign, a partnership of the federal government and the technology community. Currently, 13 federal agencies and a large number of safety organizations are partners on the website, contributing content and helping to promote and disseminate consistent messages. Since the launch of OnGuardOnline.gov and its Spanish-language counterpart AlertaenLínea.gov in September 2005, more than 12 million visitors have used these sites for information about computer security.

¹³ *NetCetera* is available online at www.onguardonline.gov/pdf/tec04.pdf.

and friendships – as well as possible legal consequences if kids create, forward, or save these kinds of messages – and gives parents straightforward advice: “Tell your kids not to do it.” With respect to cyberbullying, *Net Cetera* advises parents to talk with their kids about online behavior and about any messages or images that make them feel threatened or hurt. The guide advises parents to work with a child who is being bullied by helping them to not react, save the evidence, and block or delete the bully.

The Commission has partnered with schools, community groups, and local law enforcement to publicize *Net Cetera*, and the agency has distributed more than 3.7 million copies of the guide since it was introduced in October 2009. The FTC will continue to work with other federal agencies, state departments of education, school districts, and individual schools to distribute *Net Cetera* and OnGuardOnline.gov to parents and educators. Additionally, the FTC plans to reach out to other groups that work with kids, such as summer camps, state education technology associations, and scouting organizations to publicize these materials.

In furtherance of the FTC’s education efforts, Commission staff also participated in the Online Safety and Technology Working Group (OSTWG), a working group composed of private sector members and federal agencies. OSTWG reported its findings about youth safety on the Internet to Congress on June 4, 2010.¹⁴ Among its tasks, OSTWG reviewed and evaluated the status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, and age-appropriate labels for content. With respect to Internet safety education, OSTWG recommended greater interagency cooperation, publicity,

¹⁴ *Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group* (June 4, 2010), available at www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf.

and public-private sector cooperation for projects such as OnGuardOnline and *Net Cetera* to improve their national uptake in schools and local communities. As described above, the FTC is actively working to expand the reach of the already successful OnGuardOnline and *Net Cetera* projects.

IV. SOCIAL NETWORKING, MOBILE COMPUTING, AND P2P

In addition to education efforts to improve teen privacy, the Commission is also focused on specific technologies of which teens are particularly high users – social networking, mobile computing, and P2P file-sharing.

A. Social Networking

Social networking is pervasive among teens: 73 percent of American teens aged 12 to 17 now use social networking sites such as Facebook and MySpace, up from 55 percent two years ago.¹⁵ Nearly half of teens use these sites on a daily basis to interact with their friends.¹⁶ Teens use social networking to send messages to friends, post comments, and share photos and videos.¹⁷

The Commission has sought to protect teenage and other consumers in this environment through law enforcement, research, and education. It has brought a number of enforcement

¹⁵ See Amanda Lenhart, Kristen Purcell, Aaron Smith, & Kathryn Zickuhr, Pew Internet & American Life Project, *Social Media and Young Adults* (Feb. 2010), available at www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1.

¹⁶ See Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, *Social Networking Websites and Teens* (Jan. 2007), available at www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/More-details-from-the-survey.aspx?r=1..52

¹⁷ See Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, & Aaron Smith, Pew Internet & American Life Project, *Teens and Social Media* (Dec. 19, 2007), available at www.pewinternet.org/~media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.

actions against social networking sites since 2006, when social networking exploded on the youth scene. Most recently, the Commission announced a consent order against Twitter, Inc. settling charges that it falsely represented to consumers that it would maintain reasonable security of its system and that it would take reasonable steps to ensure that private tweets remain private. Under the order, Twitter has agreed to maintain reasonable security and to obtain independent audits of its security procedures every two years for 10 years.¹⁸ The Commission also has brought actions against several social networking sites that targeted youth but failed to adhere to the Children’s Online Privacy Protection Act (“COPPA”) with respect to users under the age of 13.¹⁹ The Commission will continue to examine the practices of social networking sites and bring enforcement actions when appropriate.

In addition to its enforcement work, the Commission has been gathering information about social networking as part of a recently-concluded series of public roundtables on consumer privacy.²⁰ The goal of the roundtables was to explore how best to protect consumer privacy without curtailing technological innovation and beneficial uses of information.²¹ Participants at

¹⁸ *In re Twitter*, FTC File No. 092 3093 (June 24, 2010) (approved for public comment), available at www.ftc.gov/opa/2010/06/twitter.shtm.

¹⁹ *United States v. Xanga.com, Inc.*, No. 06-CIV-6853(SHS) (S.D.N.Y.) (final order Sept. 11, 2006); *United States v. Industrious Kid, Inc.*, No. 08-CV-0639 (N.D. Cal.) (final order Mar. 6, 2008); *United States v. Sony BMG Music Entm’t*, No. 08-CV-10730 (S.D.N.Y.) (final order Dec. 15, 2008); *United States v. Iconix Brand Group, Inc.*, No. 09-CV-8864 (S.D.N.Y.) (final order Nov. 5, 2009).

²⁰ More information about the Privacy Roundtables can be found at www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

²¹ Several key concepts emerged from the roundtable discussions. First, participants stated that data collection and use practices should be more transparent by, for example, simplifying privacy disclosures so that consumers can compare them. Second, participants said that it should be easier for consumers to exercise choice. For example, rather than burying

the roundtables repeatedly raised issues related to social networking, and a specific panel was devoted to the subject. Experts on this panel discussed the difficulty of defining consumer expectations on social networking sites, issues related to third-party applications that use data from social networking sites, and the effectiveness of privacy disclosures and privacy settings in the social networking space.

The Commission is reviewing the information it received as part of the roundtable series and drafting initial privacy proposals, which it will release for public comment later this year.²² The Commission will consider the information it obtained about social networking as it makes its recommendations.

B. Mobile Technology

Teens' use of mobile devices is increasing rapidly – in 2004, 45 percent of teens aged 12 to 17 had a cell phone; by 2009, that figure jumped to 75 percent.²³ Many teens are using their phones not just for calling or texting, but increasingly for applications like emailing and web

important choices in a lengthy privacy policy, such choices should be presented at the most relevant time – e.g., the point of information collection or use. Further, it may not be necessary to provide choice about uses of data that are implicit or expected as part of a transaction – for example, sharing address information with a shipping company to send a product that the consumer has requested. Finally, participants noted that companies should build basic privacy protections into their systems at the outset by, for example, collecting and retaining information only if they have a business need to do so. The Commission is taking these basic principles into account as it develops privacy proposals to be released for comment later this year.

²² In addition to the information presented at the roundtables, the Commission received over 100 submissions in response to its request for written comments or original research on privacy, *available at* www.ftc.gov/os/comments/privacyroundtable/index.shtm.

²³ Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), *available at* www.pewinternet.org/~media/Files/Reports/2010/PIP-Teens-and-Mobile-2010.pdf.

browsing, including accessing social networking sites and making online purchases.²⁴ They are also using relatively new mobile applications that raise unique privacy concerns, such as location-based tracking.²⁵

The FTC has been actively addressing privacy issues relating to mobile technology for several years. In 2008, the Commission held a Town Hall meeting to explore the evolving mobile marketplace and its implications for consumer protection policy. Participants in the meeting examined topics such as consumers' ability to control mobile applications and mobile commerce practices targeting children and teens. In April 2009, FTC staff issued a report setting out key findings and recommendations based on the Town Hall meeting. Having highlighted that the increasing use of smartphones presents unique privacy challenges regarding children, the Town Hall meeting led to an expedited regulatory review of the Children's Online Privacy Protection Rule.²⁶ The review is taking place this year, even though it was originally set for 2015.

More recently, the privacy roundtable discussions devoted a panel to addressing the privacy implications of mobile computing. This panel focused on two significant issues: the extent to which location-based services were proliferating in an environment without any basic rules or standards, and the degree to which transparency of information sharing practices is

²⁴ *Id.*

²⁵ Nielsen, *How Teens Use Media* (June 2009), available at blog.nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf.

²⁶ Under the rulemaking authority granted to it by the Children's Online Privacy Protection Act of 1998 ("COPPA"), the FTC promulgated the COPPA Rule, 16 C.F.R. Part 312, in 1999.

possible on mobile devices. As with social networking, the Commission staff's upcoming report on the privacy roundtables will further address these issues.

In addition to these policy initiatives, the FTC is ensuring that it has the tools necessary to respond to the growth of mobile commerce and conduct mobile-related investigations. In the past month, the FTC has expanded its Internet lab to include smartphone devices on various platforms and carriers. The Commission also has obtained the equipment necessary to collect and preserve evidence from these mobile devices. With these smartphones, FTC staff can now improve its monitoring of unfair and deceptive practices in the mobile marketplace, conduct research and investigations into a wide range of issues, and stay abreast of the issues affecting teens and all consumers.

C. P2P File-Sharing

P2P file-sharing allows people to share their files through an informal network of computers running the same software. Teens use P2P programs to share music, games, or software online. However, P2P file-sharing presents privacy and security risks because consumers may unknowingly allow others to copy private files they never intended to share. The FTC has sought to address these risks in several ways.

First, the Commission has undertaken an initiative targeting businesses that use or allow P2P programs on their networks without implementing reasonable safeguards to protect their customers' information from inadvertent disclosure through these programs. This customer information can be leaked onto a P2P network when, for example, an employee downloads a P2P program directly onto his or her work computer, or when a business chooses to utilize P2P file-sharing programs, but does not configure its network correctly to protect such information.

To address this problem, the Commission recently sent letters notifying several dozen public and private entities – including businesses, schools, and local governments – that customer information from their computers had been made available on P2P file-sharing networks.²⁷ In the notification letters, the FTC urged the entities to review their security practices, explained that they should take steps to control the use of P2P software on their networks, and shared new business education materials designed to help them protect their confidential data from inadvertent sharing to a P2P network.²⁸ Many entities that received these notifications contacted FTC staff for additional information to aid in their investigations into the file-sharing incidents, and a number reported making changes to their security practices to prevent inadvertent file-sharing to P2P networks. At the same time it sent the notification letters, the FTC opened non-public investigations into other companies whose customer or employee information had been exposed on P2P networks.²⁹

FTC staff has also assisted P2P file-sharing software developers in devising best practices to help prevent consumers from inadvertently sharing personal or sensitive data over P2P networks. In July 2008, the Distributed Computer Industry Association published voluntary best practices to guard against inadvertent file sharing. With the assistance of an independent P2P technology expert, FTC staff have been assessing whether members are complying with these best practices.

²⁷ FTC Press Release, *Widespread Data Breaches Uncovered by FTC Probe*, (Feb. 22, 2010), available at www.ftc.gov/opa/2010/02/p2palert.shtm.

²⁸ These materials are available at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

²⁹ FTC Press Release, *supra* note 27.

The FTC also seeks to educate consumers about the risks of P2P file sharing software. Among other things, the agency provides tips for consumers about P2P in a consumer alert entitled “P2P File-Sharing: Evaluate the Risks,”³⁰ which is available through OnGuardOnline.gov, and in *Net Cetera*.

Finally, the FTC has brought enforcement actions alleging that certain P2P file sharing software providers made deceptive claims in connection with the marketing of their products.³¹

V. PRIVACY MODELS AND TEENS

The issues surrounding teens’ use of digital technology raise the question whether there should be special privacy protections for them. Some have suggested that COPPA’s protections be extended to cover adolescents between the ages of 13 and 18; others suggest that separate privacy protections should be established for teens.³²

³⁰ The consumer alert is available at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm.

³¹ *FTC v. Cashier Myricks Jr.*, Civ. No. CV05-7013-CAS (FMOx) (C.D. Cal., filed Sep. 27, 2005) (suit against the operator of the web site MP3DownloadCity.com for making allegedly deceptive claims that it was “100% LEGAL” for consumers to use the file-sharing programs he promoted to download and share music, movies, and computer games); *FTC v. Odysseus Marketing, Inc.*, Civ. No. 05-330 (D.N.H., filed Sep. 21, 2005) (suit against website operator that encouraged consumers to download free software falsely marketed as allowing consumers to engage in anonymous P2P file-sharing).

³² See Hearing: an Examination of Children’s Privacy: New Technologies and the Children’s Online Privacy Protection, Prepared Statement of Professor Kathryn Montgomery Before the Subcommittee on Consumer Protection, Product Safety, and Insurance, Committee on Commerce, Science, and Transportation, United States Senate (Apr. 29, 2010), available at www.democraticmedia.org/files/u1/2010-04-28-montgomerytestimony.pdf; see also An Examination of Children’s Privacy: New Technologies and the Children’s Online Privacy Protection Act (COPPA), Prepared Statement of Marc Rotenberg, EPIC.org, available at epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.

The COPPA statute and implementing regulations enforced by the FTC require operators to provide notice to, and receive consent from, parents of children under age 13 prior to the collection, use, or disclosure of such children’s personal information on web sites or online services. In the course of drafting COPPA, Congress looked closely at whether adolescents should be covered by the law, ultimately deciding to define a “child” as an individual under age 13. This decision was based in part on the view that most young children do not possess the level of knowledge or judgment to make appropriate determinations about when and if to divulge personal information over the Internet. The FTC supported this assessment.³³

While this parental notice and consent model works fairly well for young children, the Commission is concerned that it may be less effective or appropriate for adolescents. COPPA relies on children providing operators with parental contact information at the outset to initiate the consent process. The COPPA model would be difficult to implement for teens, as they have greater access to the Internet outside of the home than young children do, such as in libraries, friends’ houses, or mobile devices. Teens seeking to bypass the parental notification and consent requirements may also be less likely than young children to provide accurate information about their age or their parents’ contact information. In addition, courts have recognized that as children age, they have an increased constitutional right to access information and express themselves publicly.³⁴ Moreover, given that teens are more likely than young

³³ See Testimony of the Federal Trade Commission Before the Subcommittee on Communications, Senate Committee on Commerce, Science & Transportation (Sept. 23, 1998), available at www.ftc.gov/os/1998/09/priva998.htm.

³⁴ See, e.g., *American Amusement Mach. Ass’n. v. Kendrick*, 244 F.3d 572 (7th Cir. 2001) (citing *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-14 (1975); *Tinker v. Des Moines Independent School District*, 393 U.S. 503, 511-14 (1969)).

children to spend a greater proportion of their time online on websites that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.³⁵

The Commission will continue to evaluate how best to protect teens in the digital environment and take appropriate steps to do so. In specific instances, there may be opportunities for law enforcement or advocacy in this area. For example, just this week, the Commission's Bureau of Consumer Protection sent a letter to individual stakeholders in XY corporation, which operated a now-defunct magazine and website directed to gay male youth. The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information – including names, street addresses, personal photos, and bank account information from gay teens. The letter warns that selling, transferring, or using this information would be inconsistent with the privacy promises made to the subscribers, and may violate the FTC Act; thus, the letter urges that the data be destroyed.

More generally, the FTC believes that its upcoming privacy recommendations based on its roundtable discussions will greatly benefit teens. The Commission expects that the privacy proposals emerging from this initiative will provide teens both a greater understanding of how their data is used and a greater ability to control such data. Finally, the Commission is available to work with this committee, if it determines to enact legislation mandating special protections for teens.

³⁵ See *ACLU v. Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008) (citing *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007) (“Requiring users to go through an age verification process would lead to a distinct loss of personal privacy.”)); see also *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983) (citing *Butler v. Michigan*, 352 U.S. 380, 383 (1957) (“The Government may not reduce the adult population . . . to reading only what is fit for children.”)).

VI. CONCLUSION

The Commission is committed to protecting all consumers in the digital environment, especially those consumers, such as teens, who are particularly vulnerable to threats on the Internet. The FTC will continue to act aggressively to protect teens through education, law enforcement, and policy initiatives that will better enable teens to control their information online.

Thank you for this opportunity to discuss the privacy and security of teens on the Internet. I look forward to your questions.



John P. Tomaszewski, Esq.
General Counsel & Corporate Secretary
johnt@truste.com

December 15, 2011

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex E)
600 Pennsylvania Avenue N.W.
Washington, DC 20580

By Online Submission to: <https://ftcpublic.commentworks.com/ftc/2011coppafulereview/>

Re: TRUSTe Comments to COPPA Rule Review, 16CFR Part 312, Project No. P104503

TRUSTe appreciates the opportunity to comment on the proposed amendments to the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"). TRUSTe has been a FTC-approved COPPA safe harbor since 2001, and has witnessed the technological changes that the Commission references in its summary statement. We agree that the COPPA Rule should be amended to address these technological changes and that the proposed Rule changes are positive steps to streamline and provide clarity to the COPPA Rule.

We have provided specific responses to questions raised in the FTC's request for comment. In addition, we'd like to emphasize the following points:

1. *COPPA Rule changes impact both companies and end users* - It's important to assess the impact of all COPPA Rule changes from the perspective of companies that must comply, and end users (children and their parents) that might be impacted.
2. *Identifying multiple operators will remain a challenge for compliance with the Rule* - One of the significant technological changes that have impacted the COPPA Rule is the rise of online services available through an expanded array of computing devices. As a result, it is often difficult to identify which entity is the operator responsible for providing parental notice and obtaining consent. For example, including identifiers used to link the activities across different websites or online services as personal information may increase the number of instances where there will be multiple operators on a single website or online service.
3. *Industry incentives are important to promote "Privacy by Design" within a compliance framework* - TRUSTe supports the Commission's efforts to encourage "Privacy by Design" through innovation around parental consent mechanisms. TRUSTe recommends giving industry incentives to develop alternative forms of direct parental consent and privacy notices by extending the proposed Rule changes around approving alternative forms of parental consent mechanisms to also include direct parental consent and privacy notices.
4. *The COPPA Rule is strengthened by accountability and other proposed data management provisions* - TRUSTe is pleased to see the addition of accountability, security, data retention, and data management processes, as these are key components to any effective privacy program. However, there are challenges around requirements

regarding data retention and deletion being too specific or prescriptive. Providing specifics around data retention timeframes could potentially conflict with the operator's other legal obligations.

5. *The COPPA safe harbor program is strengthened by additional requirements for safe harbor programs* - Operators need to be accountable to their stated privacy promises and meet program requirements of any approved safe harbor program in which they participate. Approved safe harbor programs must also be accountable around how they administer their programs. Additional criteria for safe harbor approval, reporting around program compliance, and requiring annual recertification are important. Such criteria will further demonstrate why COPPA safe harbors serve as a model for other types of safe harbor programs, and why these types of program are effective.

To respond to the Commission's questions, TRUSTe has provided use case examples, along with specific recommendations that address each of the five key areas of proposed Rule changes:

1. Definitions
2. Notice
3. Parental Consent
4. Data Retention and Deletion
5. Safe Harbors

1. Definitions

Question 4: Are there identifiers that the Commission should consider adding to the list of "online contact information"?

TRUSTe supports the addition of "geo-location" data to the definition of personal information. Under its Privacy Certification program, TRUSTe classifies geo-location data as sensitive personal information.¹ TRUSTe's program requirements define geo-location data as "information obtained through an Individual's use of a Mobile Device and is used to identify or describe the Individual's actual physical location at a given point in time." A key component of this definition is the qualifier "actual physical location" that references the technical capabilities of the device to pinpoint the actual physical location of an individual.

We believe it is important to qualify the definition of geo-location data to differentiate it from other types of location data, depending on the ability of the device or software to pinpoint actual physical location. For example, certain geo-location information, such as a zip code, may not reflect a child's actual location. Location identifiers, such as address, city, and zip code that are directly provided by the child are already covered under the definition of Personal Information under the Rule. What is not currently reflected in this definition is the ability of certain data, such as geo-location data, to identify the child's precise location.

TRUSTe recommends that the Commission amend the definition of "Personal Information" under the Rule as follows:

Personal information means individually identifiable information about an individual

¹ TRUSTe, Program Requirements, 18 Nov. 2011, <http://www.truste.com/privacy-program-requirements/program-requirements>.

collected online, including: ...

(j) Precise geo-location data that can be used to identify a Child's actual physical location at a given point in time.

TRUSTe has determined it prudent to describe personal information in a more effects-based mode, rather than attempting to describe what specific data points constitute personal information. Much of this approach is based on the observation that data may or may not be personal information depending on the context of the data relative to other data (or meta-data). In addition to the example noted above, depending on the actual value of the data, it may be personal information in one context where it is not in another (e.g. first name, last name, ZIP may be personal information if the specific ZIP only has one combination of first and last name).

Question 5: Proposed § 312.2 would define personal information to include a "screen or user name."

- a. What would be the impact of including "screen or user name" in the definition of personal information?*
- b. Is the limitation "used for functions other than or in addition to support for the internal operations of the website or online service" sufficiently clear to provide notice of the circumstances under which screen or user name is covered by the Rule?*

The above-referenced changes to the Rule, including the limitations around "used for functions other than to support for the internal operations of the website or online service," do not effectively reflect current uses of screen or user name by a single operator and do not provide sufficient notice of when screen or user names are covered by the Rule. The following use cases demonstrate why:

1. A single operator operates multiple websites or online services that are integrated in such a way that a child can easily navigate from one website or online service by only having to login once. Information collected from the child includes screen or user name and password, and the operator's privacy policy is the same across all the websites or online services. Will the operator need to obtain parental consent for the child to access each website or online service? What impact would this have on the end user experience?
2. A single operator offers mobile optimized versions of its PC website or online service. The operator offers a mobile application that utilizes the same screen or user name the child uses to access the website or online service on the desktop web. The child's activities are synched up regardless of which device she or he uses to access the website or online service. For example, if a child is playing a game on a laptop and later logs into the game through the mobile app, the child will pick up where she left off, and content is displayed based upon her settings. Will the parent only need to provide consent once so that consent will apply to all forms of a website or online service regardless of how it is accessed (e.g. website or mobile application)?
3. An operator operates a website or online service that enables children to connect with each other in virtual worlds. The child is asked to create a screen name so they can chat with others in the virtual world. The chat function filters out words considered to be personally identifiable. Along with screen name the operator collects age and gender to allow the child to customize her avatar and to place the child into age appropriate worlds

to ensure the child is chatting with others her own age. Will screen or user name be considered personal information if combined with other non-personally identifying information such as age and gender? This may impact an operator's ability to segregate users into age appropriate groups, and may also complicate its ability to provide personalized online experiences.

4. A web-connected gaming console enables gamers, including children, to play against each other, chat, and post high scores. Players are recognized by screen or user name. The game's chat function filters out words considered to be personally identifiable. The screen or user name is used for all games available for that gaming console. Will the web-connected gaming console -where a screen or user name is used within a single gaming console but across multiple games - be considered a single online service, or will the games that the child plays each be considered a separate online service?

The Commission notes in its discussion that while screen and/or user names are becoming increasingly portable, the addition of screen or user names to the definition of personal information does not effectively address the issue of portability.² Operators offering a suite of related websites or online services that utilizes a single screen or user name throughout the service offerings intend the child to only be recognized within that suite of services so the child may have a seamless online experience. TRUSTe believes placing restrictions around providing a centralized registration and login across all services will provide a poor online experience. TRUSTe recommends modifying when a screen or user name is personal information to address the use case noted in the Commission's discussion - the case of being able to identify a child by screen or user name across multiple services provided by multiple operators.

The Commission should also consider expanding the definition of website or online service to include a set of websites or online services integrated through a common registration or login process offered by a single operator.

Question 6: Proposed § 312.2 would define personal information to include a "persistent identifier."

- a. *What would the Impact of the changes to the term "persistent identifier" be in the definition of personal information?*
- b. *Is the limitation "used for functions other than or in addition to support for the internal operations of the website or online service" sufficiently clear to provide notice of the circumstances under which a persistent identifier is covered by the Rule?*

Persistent identifiers differ from screen or user name because a screen or user name is something that is typically created by the user. A persistent identifier is an identifier that is automatically created by the party setting the identifier such as an IP address or a number contained in a cookie. A screen or user name identifies an individual, whereas a persistent identifier identifies a browser or a device. We think that this is an important distinction when considering whether persistent identifiers should be classified as personal information. We also

² "Data Portability Definitions," [Data Portability Project](http://wiki.dataportability.org/display/archive/DataPortability+Definitions), 21 Nov. 2008, 12 Dec. 2011, <http://wiki.dataportability.org/display/archive/DataPortability+Definitions> and Christian Scholz, "What is Data Portability," mrtopf.de, 12 March 2008, 12 Dec. 2011, <http://mrtopf.de/blog/data-portability/what-is-data-portability/>

believe that including persistent identifiers in the definition of personal information will hinder a single operator's ability to offer users rich online experiences. The following use cases illustrate this proposition:

1. An operator may use a persistent identifier (e.g. GUID) to track a child-user within its websites and online services. This tracking enables the operator to maintain the child's session (e.g. recognize logins, etc.), personalize the child's experience, and gather analytics about which areas of the websites or online services are used. The tracking is limited to the websites and online services offered by that single operator, and does not track the child's activity after she navigates to a web site or online service offered by another operator.

The operator may use a third party analytics service to track web site or online service use as described in the above paragraph. Will the third party analytics service also be classified as an operator if it is only tracking usage activity within a group of websites or online services offered by a single operator? We think that tracking by an operator, or a third party acting on behalf of the operator, across a group of multiple websites or online services provided by the same operator, is not sufficiently addressed in the proposed change to the term "persistent identifier."

2. An operator may also use a persistent identifier to recognize a child-user when they access the website or online service from different devices such as laptop, tablet, or smartphone. The operator is able to offer the child a seamless experience, displaying content based upon the child's set preferences, or to display the last game level the child was playing so she can pick up where she left off. Using an identifier to provide a seamless online experience when accessing the same website or online service through different devices needs to be addressed.

TRUSTe recommends that persistent identifiers not be included as part of the definition of personal information, but be defined separately. A persistent identifier by itself is not personal information as it does not allow you to contact a discrete individual but rather is assigned to a device or similar technology. However, when a persistent identifier is combined with other data that allows for the identification and contacting of a discrete individual, then the combined data may be personally identifiable.

The standalone definition of persistent identifier should include language stating that if the persistent identifier is combined with other data that enables the online contacting of a child, that combined data is personal information.

Question 7: Proposed § 312.2 would define personal information to include "an identifier that links the activities of a child across different websites or online services." Is the language sufficiently clear to provide notice of the types of identifiers covered by this paragraph?

TRUSTe agrees that tracking a child's activities across different websites or online services over time for the purpose of serving the child behaviorally targeted advertisements, or to build a profile about the child that is made available to third party marketers warrants a greater level of privacy protection. As with others in the industry, we recognize that information collected from

children is sensitive and requires greater protections.³ If entities engage in online behavioral advertising directed to children, and they have actual knowledge that these children are under the age of 13, those entities must comply with the COPPA Rule as well as guidance from the FTC's Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting and Technology.

Classifying “an identifier that links the activities of a child across different websites or online services” as personal information will serve to provide a poor user experience for both children and parents, and will not provide greater privacy protections.

An example would be a website or online service offering free games for children that does not collect personal information, but partners with a third party analytics provider to collect aggregated data about its users including how the user got to the website or online service, and where the user went after they left the website or online service. To collect the data, the analytics provider uses an identifier to gather the information. Under the proposed definition, the analytics provider would be required to obtain parental consent prior to collecting information from the child. This scenario raises some questions:

1. Is the analytics provider an operator? In some cases the identified third party operator will not have a direct relationship with or explicitly request personal information from consumers. In these cases, the first party operator is responsible for obtaining parental consent since the first party has the direct relationship. It's not appropriate for the third party to insert themselves between the consumer and the first party operator.
2. Will the parent need to provide new consent each time a new “operator” appears on a website or online service?
3. What would the notice – consent experience look like in the case of multiple operators? Will each “operator” have to ask the child for the parent's email address for the purpose of sending notice and obtaining consent? This will require companies that traditionally do not have a direct relationship with users, or who have not requested personal information directly from a user, to now collect personal information from a child. Additionally this could be cumbersome in the case of a mobile device. The third party should be allowed to rely on the consent obtained from the first party operator where the third party is “operating” under the direction of the first party.
4. How would consent be tracked? This would raise issues similar to those raised around honoring opt-outs. In a cookie-based system, if a child or parent clears their cookies or uses in-private browsing, the child and parent's preferences, including parental consent are removed. Would this retrigger notice-consent?

TRUSTe recommends that the Commission does not add include “an identifier that links the activities of a child across different websites or online services” to the definition of personal information, because this type of identifier does not identify a discrete child. It is when this data is combined with other data from third party sources that permits the identification of a child. Linking activities across multiple sites identifies a browser or device. Also, this should not be

³ The DAA's OBA principles, based on the FTC's own Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting and Technology exemplify this approach. “About the Self-Regulatory Principles for Online Behavioral Advertising,” 18 Nov. 2011 <http://www.aboutads.info/obaprinciples>.

added for the reasons cited above. Trying to meet this standard is a risk operators most likely will be reluctant to take on, and would likely chill innovation.

Question 8: Proposed § 312.2 would define personal information to include “photograph, video, or audio file where such file contains a child’s image or voice” and no longer requires that photographs (or similar items) be combined with “other information such that the combination permits physical or online contacting.” What would be the impact of expanding the definition of personal information in this regard?

This proposed change will impact social sites that enable children to communicate with others using a screen name, without the collection of any other identifying information, and offer features that allow the child to upload user generated content.

Operators that allow children to upload user-generated content under the current rule exception will need to provide notice and obtain consent prior to allowing the further uploading of user-generated content. It is unclear whether the operator will need to remove user-generated content uploaded under the current Rule, where no other identifying information is associated with that content, or whether that material would be grandfathered in.

TRUSTe agrees biometrics such as those provided in a photo, video, or audio recording are personal information and greater protections need to be provided in light of technologies such as facial recognition technology services becoming more widely available. TRUSTe recommends that notice and consent be provided on a going-forward basis. User generated content uploaded by a child prior to release of a final updated Rule should be grandfathered under the current Rule thus not requiring operators to delete the content.

Question 9b: Does the combination of date of birth, gender, and zip code provide enough information to permit the contacting a specific individual such that this combination of identifiers should be included as an item of Personal Information?

Studies have shown that the combination of date of birth, gender, and zip code can identify a discrete individual.⁴ However, much of these three data points capability to be personal information depends on the context of the data. These three data points usually need to be combined with data from another source in order to contact that discrete individual.

Operators collect date of birth, gender, and zip code to provide a personalized experience for their users. For example, operators providing services that enable children to connect and interact with each other collect this type of data, along with screen or user name, to allow the child to create a profile so the child can interact with others that are of similar age and share similar interests.

Combining information collected from the child with another piece of information that the operator uses to contact the child or the child’s parents should be added to the definition of personal information along with an exception around providing requested services. If the Commission adds date of birth, gender, and zip code to the definition of personal information, TRUSTe recommends the added subsection of the definition to read:

⁴ Prof. Paul Ohm, “Public Comment to the Federal Trade Commission, Re. COPPA Rule Review P104503,” [University of Colorado Law School](http://www.ftc.gov/os/comments/copparulerev2010/547597-00040-54850.pdf), 30 June 2011, 18 Nov. 2011, <http://www.ftc.gov/os/comments/copparulerev2010/547597-00040-54850.pdf>.

“date of birth, gender, and zip code combined with an identifier and where such combined information is used for functions other than or in addition to support for the internal technical operations of the website or online service”.

Question 9c: Should the Commission include “Zip + 4” as an item of Personal Information?

“Zip + 4” by itself is not enough to identify a discrete individual and would need to be combined with other data points to identify, locate, or contact an individual and should not be added to the definition of personal information.

Question 11a: Is the term “activities to maintain the technical functioning” sufficiently clear to provide notice of the types of activities that constitute “support for the internal operations of the website or online service”? For example, is it sufficiently clear that the mere collection of an IP address, which is necessary technical step in providing online content to web viewers, constitutes an “activity necessary to maintain the technical functionality of the website or online service”?

The term “activities to maintain the technical functioning” does not take into consideration third party services that may be used to assess usability of the website or online service such as understanding how individuals interact with a website or online service (e.g. analysis of which areas or features are most popular, etc.).

TRUSTe recommends the Commission re-assess the definition of “support for the internal operations of website or online service” as this definition is limiting and does not effectively define what is meant by “support for the internal operations.” It is unclear why “or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4)” is called out specifically in the definition and the other allowable exceptions permitted under §§ 312.5(c) or services the parent has consented to are not included.

The Commission should consider revising the definition to read

Support for the internal operations of the Web site or online service means those activities necessary to maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, or to fulfill a request of a child as permitted by § 312.5(c), and the information collected for such purposes is not used or disclosed for any other purpose either by the Operator or a person who provides support for the internal technical operations of the Web site or online service.

2. Notice

Question 12: Do the proposed changes to the “notice on the website or online service” requirements in § 312.4(b) clarify or improve the quality of such notice?

TRUSTe supports the Commission’s goal of streamlining the requirements around notices to parents, as well as making the notices easier for parents to read and understand. TRUSTe agrees with the Commission’s proposal to remove the requirement around operators having to state “that the operator may not condition a child’s participation in an activity on the child’s disclosing more personal information than is reasonably necessary to participate in such activity” (§ 312.4(b)(2)(v)). This is a practice an operator should be required to comply with rather than a required disclosure.

However, the proposed changes to § 312.4(b) do not clarify or improve the quality of the notice, specifically:

- (1) *Each operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and email address;*
- (2) *A description of what information each operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,*

In the discussion, the Commission notes that the change from listing contact information for a single operator to requiring the notice to list contact information for all operators will help parents find "...the appropriate party to whom to direct any inquiry". TRUSTe's opinion is that the listing of contact information for all operators will serve to confuse parents, and cause frustration (for example in the case where an operator's contact information is out-of-date or is unresponsive to a parent's inquiry). This will also require operators to constantly update their privacy notice as third party partnerships, relationships, or service providers change; thus making it a challenge for operators to maintain up-to-date accurate notices.

TRUSTe recommends the Commission maintain the current requirement around allowing a single operator to be designated as a point of contact in the case where there are multiple operators for a single website or online service. Note that such primary, or "first party" operator will have to retain responsibility for the notice and consent process for all "third party" operators "operating" under the first party operator's instruction.

The requirement of "...what information each operator collects..." will serve to continue to make notices onerous documents for parents to navigate, especially on a mobile device, as they try to figure out who each operator is and what it does with collected data. This does not meet the Commission's goal of streamlining the notice. As the Commission is aware, privacy notices are challenging to read as most privacy notices are typically written by someone with a legal background, and at a college reading level. A recent Law.com article by Paul Bond and Chris Cwalina notes:

The average adult in the United States reads at an eighth-grade level. Shannon Wheatman, Ph.D., a notice expert with Kinsella Media, LLC, recently reviewed the privacy policies of 97 Fortune 100 companies. (Three Fortune 100 companies have no privacy policies.) Wheatman found that on average, Fortune 100 companies drafted privacy policies at the reading level of a junior in college, well beyond general comprehension.⁵

TRUSTe recommends § 312.4(b)(2) to be revised to read:

- (2) *A description of what information is collected from children through the website or online service, including whether the website or online service enables a child to make personal information publicly available; all uses of such information, and; the operator(s)' disclosure practices for such information*

⁵ Paul Bond and Chris Cwalina, "Making Your Privacy Policy Comprehensive and Comprehensible," Corporate Counsel, 1 Sept. 2011, 18 Nov. 2011, <http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202512963808>.

Streamlining and simplifying notices can be done through how the notice is designed, as described further below.

Question 14: Should the Commission modify the notice requirement of the Rule to require that operators post a link to their online notice in any location where their mobile applications can be purchased or downloaded (e.g. in the descriptions of their application in Apple's App Store or in Google's Android Market)?

TRUSTe's Trusted Download Program requires its program participants to provide primary notice regarding what the software does (e.g. whether it tracks or will display ads), and access to other notices such as a privacy policy prior to the consumer consenting to installing the software.⁶ A similar concept should be applied to mobile applications. Consumers should be able to make an informed decision on whether to install the mobile application including having access to the privacy policy.

TRUSTe supports adding the qualifier- "*any location where mobile applications can be purchased or otherwise downloaded*" - to the COPPA Rule notice requirement.

Question 15: Are there other effective ways of placing notice that should be included in the proposed revised Rule?

The proposed Rule changes will streamline the requirements for direct notices to parents, and recognize that relying on parents to comprehend a long privacy policy may not be the most effective way to get them the information they need to make an informed decision about their child's online activities. On November 30, 2011, TRUSTe released the results of its review of the privacy policies for the top Alexa 100 websites. We found on average privacy policies are 2462 words long and takes the average consumer about 10 minutes to read.⁷ Simply put, consumers do not read privacy policies because they are too complicated and long.

TRUSTe has been exploring privacy policy design in order to make privacy policies easier for consumers to read by using simplified language and iconography to guide consumers. As part of that work, TRUSTe has developed a short notice design for both website and mobile privacy policies, boiling policies down to what consumers really want to know. These design concepts can be adapted to the direct notice and privacy policy requirements of the COPPA Rule.⁸

TRUSTe recommends the Commission require that the parental direct notice or the operator's privacy policy be optimized for the device it's displayed on. This can be done based upon screen size of the device so it is not platform specific, and should not place an undue burden on companies to support. Parents are then provided effective notice and can easily find the information they are looking for.

⁶ TRUSTe, *Program Requirements*, 18 Nov. 2011,

http://www.truste.com/pdf/Trusted_Download_Program_Requirements_Website.pdf.

⁷ Devin Coldewey, "Examination of Privacy Policies Shows a Few Troubling Trends," *TechCrunch*, 30 Nov. 2011, 12 Dec. 2011, <http://techcrunch.com/2011/11/30/examination-of-privacy-policies-shows-a-few-troubling-trends> and similar finding at "Privacy Policy Infographic," *Selectout Privacy Blog*, 28 Jan. 2011, 18 Nov. 2011, <http://selectout.org/blog/privacy-policy-infographic/>.

⁸ "Layered Policy Design," *TRUSTe Blog*, 20 May, 11 Nov. 2011, <http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/> and "Short Notice Privacy Disclosures," *TRUSTe Blog*, 23 May, 11 Nov. 2011, <http://www.truste.com/blog/2011/05/23/short-notice-privacy-disclosures/>.

TRUSTe would also like to see the Commission encourage innovation in improving how direct parental notices and privacy policies are presented in the same way the Commission is encouraging innovation around developing alternative forms of parental consent.

3. Parental Consent

Question 19: The Commission proposes eliminating the “email plus” mechanism of parental consent from § 312.5(b)(2). What are the costs and benefits to operators, parents, and children of eliminating this mechanism?

Email Plus is not an effective method for obtaining verifiable parental consent. The mechanism can be easily “gamed” by the child and is not effective in providing the parent direct notice regarding the operator’s data collection practices. TRUSTe has long held this view and has never allowed Email Plus under its Children’s Online Privacy certification program.⁹ At a minimum, parental consent mechanisms should verify that the person providing consent is an adult. TRUSTe encourages taking consent mechanisms one step further by verifying the person providing consent is a parent or guardian authorized to provide consent.

Question 20: Proposed § 312.5(b)(3) would provide that operators subject to Commission-approved self-regulatory program guidelines may use a parental consent mechanism determined by such safe harbor program to meet the requirements of § 312.5(b)(1). Does proposed § 312.5(b)(3) provide a meaningful incentive for the development of new parental consent mechanisms?

TRUSTe encourages allowing safe harbor programs to approve parental consent mechanisms, as they will encourage innovation around alternative mechanisms or technologies for obtaining parental consent, while also improving the notice-consent experience for both child and parent.

One frustration that TRUSTe has observed among operators, is that current consent mechanisms require the child to leave the website or online service to go get the parent or stop using the website or online service until the parent checks their email to take additional steps. Clearly, there is opportunity here for operators to innovate around providing an improved experience.

It has been TRUSTe’s experience that operators like to engage with the safe harbors early in the product development cycle. TRUSTe has worked with a number of operators - both start-ups and established businesses - and helped them review their parental consent mechanisms at different stages of the development cycle. It is a cost benefit to operators to engage early in having an outside party review the parental consent mechanism starting at either the design or wireframe stage.

4. Data Retention and Deletion

Question 22b. Should the Commission propose specific time frames for data retention and deletion?

In February 2011 TRUSTe updated its privacy certification program requirements with a specific provision requiring that clients state in their privacy policies how long they retain collected

⁹ TRUSTe, “COPPA Program Requirements,” 18 Nov. 2011, http://www.truste.com/pdf/Childrens_Privacy_Seal_Program_Requirements_Website.pdf.

data.¹⁰ This program change generated questions from clients regarding how specific their privacy policies need to be regarding data retention.

Companies will face challenges complying with a specific timeframe requirement because the requirement could potentially conflict with other legal obligations such as statutes of limitation. A second challenge is the length of time of the relationship between child users and the operator may vary. For example, how long data is retained may depend on the child's continued engagement with the operator's website or online service. The operator may choose to deactivate a child's account or login due to a period of inactivity, or if a parent requests the operator to delete the child's information. Lastly, data retention policies may vary among business models depending on the type of data that is collected and the shelf life of that data. For example, links provided through social media outlets have a shelf life of only three hours.¹¹

TRUSTe recommends the Commission not be too prescriptive in proposing data retention timeframes. Rather, we support having operators disclose what their data retention policies are in their privacy statements. In the alternative, TRUSTe recommends the Rule allow the privacy statement to disclose a retention period that is "...necessary to meet the [operator's] legal obligations. Also, guidelines in the COPPA FAQs would be more useful in this context rather than providing specific timeframes in the Rule itself.¹² In the past the Commission has used the COPPA FAQs to provide guidance regarding specific business use cases and these can be updated as new business use cases arise rather than making a change to the Rule itself.

5. Safe Harbors

Question 23: Proposed § 312.11(b)(2) would require safe harbor program applicants to conduct a comprehensive review of all member operators' information policies, practices, and representations at least annually. Is this proposed annual review requirement reasonable? Would it go far enough to strengthen program oversight of member operators?

While TRUSTe generally supports safe harbor audits, we feel that this particular requirement is unclear. Specifically, it is unclear whether this annual review is an evaluation of whether the operator has changed their practices (or not), or whether the review is a complete re-processing of the original certification of the operator's practices. TRUSTe uses certification coupled with ongoing monitoring to verify that an enrolled operator's privacy practices, consent mechanisms, and privacy policies have not changed since initial certification.

If a safe harbor is conducting ongoing monitoring throughout the annual certification period, then a complete re-certification of the operator's practices is not necessary as the safe harbor is aware of the operator's practices throughout the certification period. Annual re-certification, which includes reviewing the privacy policy, direct notice to parents, and the parental consent mechanism should verify that the operator's practices have not changed. Focusing on whether changes have been made since initial certification versus a full certification annually is much more scalable for the safe harbor to manage a growing program, so long as there is on-going monitoring as part of the safe harbor's processes.

¹⁰ TRUSTe, *Program Requirements*, 18 Nov. 2011, <http://www.truste.com/privacy-program-requirements/program-requirements>.

¹¹ "You just shared a link. How long with people pay attention?" *Bitly Blog*, 6 Sept. 2011, 18 Nov. 2011, <http://blog.bitly.com/post/9887686919/you-just-shared-a-link-how-long-will-people-pay>.

¹² "Frequently Asked Questions about the Children's Online Privacy Protection Rule," 7 Oct. 2008, 18 Nov. 2011, <http://www.ftc.gov/privacy/coppafaqs.shtm>.

Question 24: Proposed § 312.11(c)(1) would require safe harbor program applicants to include a detailed explanation of their business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of member operators' fitness for membership in the safe harbor program. Is this proposed requirement reasonable? Would it provide the Commission with useful information about an applicant's ability to run a safe harbor program?

TRUSTe supports requiring safe harbor applicants to provide a detailed explanation of their business model, certification processes, and technical capabilities around administering a COPPA safe harbor program. It is important for self-regulatory programs to demonstrate impartiality, and show they use multiple methodologies (e.g. self-attestation, human review, and technology) to assess the level of an operator's compliance with the safe harbor's program standards. The approaches used to conduct certification, ongoing monitoring and re-certification needs to be balanced so the safe harbor is not heavily relying on any one methodology (e.g. self-attestation). Applicants should also include information regarding reporting that the safe harbor will provide enrolled operators regarding program compliance and frequency of that reporting.

Question 25a: Should the Commission consider requiring safe harbor programs to submit reports on a more frequent basis, e.g., annually?

TRUSTe supports requiring safe harbors to report on their programs annually. From a business standpoint, we believe that this requirement is more manageable and can be synced up with other annual reporting obligations. TRUSTe generates reports regarding program compliance for its U.S. – E.U. Safe Harbor Program on an annual basis and feels this would not be an unreasonable reporting frequency.

TRUSTe recommends annual reports be submitted within three months after the annual reporting period. For example for the reporting period Jan 1, 2012 – Dec 31, 2012 the report is submitted by March 31, 2013.

At this time, it is unclear which program metrics are to be reported to the Commission. Specifically, we think it's important to clarify whether COPPA reporting will include alleged program violations or focus on verified program violations. TRUSTe recommends that reporting be limited to uncured, verified program violations and aggregate metrics on the overall program rather than those pertaining to a specific operator. This preserves incentives for operators to stay within the COPPA safe harbor program.

Reporting on verified violations will provide the Commission more useful data regarding the safe harbor's effectiveness around managing its program. Requiring reporting of unverified and uncured violations by a specific operator will be a strong disincentive for any company to join a safe harbor program. The goal of reporting is to hold safe harbors accountable for properly administering their programs including demonstrating they are monitoring the practices of enrolled operators. This can be done without having to name the specific operator found in violation of the program. For example, reporting provided by the safe harbors could include:

- Total number of enrolled operators
 - Change from previous reporting period
- Total number of websites URLs or online services (e.g. mobile apps)
 - Change from previous reporting period

- Total number of program violations found and resolved
 - Total discovered through program monitoring
 - Total reported through a consumer feedback mechanism
- Breakdown by violation type and resolution (e.g. operator immediately corrected violation)
 - Failure to obtain parental consent prior to collecting personal information from a child
 - Personal information collection practices that do not fall under an allowable exception
 - Direct notice to parents missing required disclosures
 - Privacy policy missing required disclosures
 - Violation of certified privacy policy
 - Disclosure of a child's personal information to a third party without parental consent
 - Changed direct notice to parents or privacy policy without prior review by safe harbor
 - Materially changed practices without providing new notice and obtaining parental consent
 - Link to privacy policy not present
- Approval of alternative parental consent mechanisms
 - Outline what was approved and why it meets the requirements of the Rule

Question 25b: Should the Commission require that safe harbor programs report to the Commission a member's violations of program guidelines immediately upon their discovery by the safe harbor program?

As noted above, reporting requirements for the safe harbor programs need to balance two goals: providing the Commission assurances the safe harbors are monitoring the practices of their enrolled operators, while also giving operators incentive to join a COPPA safe harbor program. The annual report can include information on the types of program violations the safe harbor found during the reporting period and how these violations were handled.

It is not clear if the Commission is looking for immediate reporting on all verified program violations, or intentional violations where the operator has taken an action to violate the program. TRUSTe recommends the Commission limit required immediate reporting to intentional program violations. If all program violations are reported there will be a significant amount of "noise" the Commission will need to sift through to understand the data. The safe harbors are best equipped to make the determination if a violation is intentional versus a simple mistake.

The safe harbors need some flexibility to investigate and work with their certified operators to understand the scope of the violation (e.g. number of users affected), and work with operators to determine what needs to be corrected, the best approach for correcting the violation, and the timeframe in which to correct it.

To effectively investigate reported violations (e.g. through a consumer feedback mechanism) or discovered violations quickly, a safe harbor needs to engage with the operator upon discovery. Part of the process for reviewing reported violations is to replicate the consumer's reported experience. It may take time to replicate a reported violation through testing which would warrant deeper investigation. For example, when TRUSTe receives reports of sharing email

addresses with third parties without the consumer's consent, TRUSTe will perform email seeding to confirm there is a violation.¹³

Immediate reporting may not always be possible or prudent. In TRUSTe's experience, when program violations are found, its clients typically resolve found violations fairly quickly, at times in a matter of just a few days.

More importantly, immediate reporting by a safe harbor to the Commission of program violations could become a disincentive for companies to join a safe harbor program. There may be concerns by companies that reported violations would trigger further investigation by the Commission, and invite unwanted scrutiny that a company may not otherwise encounter, which is why TRUSTe recommends immediate reporting of only intentional program violations.

Reporting on a per incident basis may also hinder the safe harbor's investigative process by adding more steps to that process, and potentially impact the ability for the safe harbor to scale that process. By way of example - in 2010, TRUSTe received, reviewed, and processed over 7,700 consumer complaints. Out of those complaints, just 12% required the client to take action ranging from revising their privacy policy to changing data collection practices. TRUSTe uses the same process for investigating consumer complaints across all its certification programs so it is consistent (e.g. both clients and consumers know what to expect), and scalable (meaning the process can support an increase in volume as the number of TRUSTe certified companies grows).

TRUSTe appreciates the opportunity to provide comments on the proposed changes to the COPPA Rule and supports the overall direction of the Commission to provide continued privacy protections for children in light of emerging technologies.

TRUSTe hopes the Commission will consider the use cases and examples outlined above in thinking through the challenges and complexities around implementing the Rule changes as currently proposed.

For questions regarding these comments, please contact Joanne Furtch, Director of Product Policy, at jfurtch@truste.com.

Sincerely,

John P. Tomaszewski
General Counsel and Corporate Secretary

¹³ ¹³ Email Seeding: TRUSTe creates multiple unique e-mail addresses and subscribes them via the client's site, using domain names and other information that do not indicate a connection to TRUSTe. An alert is triggered if a seed address receives further e-mail after the unsubscribe request should have taken effect, helping to monitor on-going unsubscribe compliance.



Why Your App Must Comply With Child Privacy Regulations

Alysa Z. Hutnik is a partner in the Advertising & Marketing and Privacy & Information Security practices at [Kelley Drye & Warren, LLP](#). Her co-author, [Matthew P. Sullivan](#), is an advertising and privacy associate at Kelley Drye & Warren, LLP. Read more on Kelley Drye's advertising law [blog](#) Ad Law Access, or keep up with the group on [Facebook](#) and [Twitter](#).

Earlier this week, the Federal Trade Commission (FTC) announced a settlement with mobile app developer [W3 Innovations, LLC](#) (W3) and its president, Justin Maples, over [alleged children's privacy violations](#). The FTC action was intended to send a message to the mobile app market that it will be closely monitoring the industry for business practices that violate consumer protection law, including privacy restrictions.

While the case marks the FTC's first enforcement action against a mobile app developer, it won't be the last. Earlier this year, Jessica Rich, deputy director of the FTC's Bureau of Consumer Protection [testified](#) to Congress that the agency has "a number of active investigations into privacy issues associated with mobile devices, including children's privacy." If you're in the business, and your mobile app fails to identify and comply with laws regarding privacy and disclosure requirements, your company might find itself defending an investigation by the FTC. Not only does that situation involve heavy cost, but an investigation will put your business and its reputation at risk.

Furthermore, if your app either intentionally targets or is attractive to kids, the FTC is even more likely to scrutinize. A recent [report](#) finds that games and social networking activities — both hugely popular with kids — comprise two of the three most popular mobile app categories. The market is expected to reach \$3.8 billion by the end of 2011. As more developers position their apps to capture a piece of the pie, the settlement with W3 warns that a casual approach to legal compliance can mean downfall.

FTC Takes Issue With W3 App's Collection of Children's Information

Better known as [Broken Thumbs Apps](#), W3 creates and sells the popular "Emily Apps," including *Emily's Girl World* and *Emily's Runway High Fashion*. Both were available through the "Games-Kids" section of Apple's App Store. The apps encouraged children to send emails to "Emily" that included shout-outs to friends, pet photographs and requests for advice. According to the FTC, the emails were then posted as public entries to "Emily's blog," accessible through all of the Emily App sites. Children also could submit responses to the blog

Mashable

entries using a standardized comment form that required them to release their names and email addresses.

The FTC alleged that the Emily Apps features violated the [Children's Online Privacy Protection Act](#) (COPPA) because the personal information of children under age 13 was collected without parental consent. The rule has two key requirements:

- **Don't Overlook the Privacy Policy:** You must prominently post a privacy policy on your homepage, as well as anywhere on your site or app where you collect information from kids. The privacy policy must clearly explain the type of information, how it's collected, how it's used, whether the information is disclosed to third parties, and the procedures parents can take to refuse, review or remove their children's information from the site.
- **Parental Consent is Key:** You must notify parents and get their consent *before* you collect, use or disclose a child's personal information.

Fair warning: even if you don't think your app targets kids, the FTC may still determine a general audience app is subject to these requirements if the app is used by a significant number of children.

App Developer Enters 20-Year FTC Settlement

The FTC has a range of tools to address and remedy practices that violate privacy and other consumer protection laws. In the 20-year settlement with W3 and its president, the FTC requires the company to take the following actions:

- Delete all personal information that W3 obtained through the Emily Apps
- Pay a civil penalty of \$50,000
- Avoid future violations of the privacy rule

For years, the FTC will monitor the app developer and its president, Justin Maples, to confirm they are complying with the settlement. The company will also have to submit records and compliance reports to the FTC for multiple years going forward. If they violate the settlement at any point over the next 20 years, the company could incur additional monetary penalties of up to \$16,000 for each violation of a settlement provision.

W3 is the latest in a growing list of companies in the mobile app space (including [Apple](#), [Google](#) and [Pandora](#)) to attract unwanted scrutiny over its handling of consumer information. This latest case shows that the issue is escalating, and the failure to address it can be very costly. Given the FTC's interest, companies seeking to enter the mobile app market or to engage a younger audience via games, for example, should be aware of the [key considerations and best practices](#) to help reduce the risk of legal and regulatory scrutiny.



4 Legal Considerations for Building a Mobile App

Alysa Z. Hutnik is a partner in the Advertising Law and Privacy & Information Security practices at [Kelley Drye & Warren LLP](#). Her co-author, [Christopher M. Loeffler](#), is an advertising and privacy associate at Kelley Drye & Warren LLP. Read more on Kelley Drye's advertising blog [Ad Law Access](#) or keep up with the group on [Facebook](#) or [Twitter](#).

If creating a mobile app is next on your business agenda, you're not alone. A recent [report](#) pegs mobile app revenue from the four major application stores at \$2.1 billion in 2010. Revenue is forecast to grow a staggering 77.7% in 2011 to \$3.8 billion, and smartphone adoption rates continue to increase.

Whether your app is destined for an *Angry Birds*-like following or will serve a more niche market, your development checklist should address traditional legal items for a new business venture. Given the broad consumer audience that comes with many mobile apps, it's helpful to keep in mind the types of issues tracked closely by the consumer protection bar, consumer advocates, regulators and private litigants.

Their scrutiny essentially boils down to two core questions:

- Are there any unexpected (bad) surprises connected with your app from a user experience — namely, does the app clearly convey all potential monetary charges (both initial download and in-app options)?
- What information from the user and the device will be collected and shared with others, and was that clearly disclosed and consented to before data was collected/shared?

Failure to identify and address these issues can result in complaints and negative media coverage and quickly turn positive app buzz into formal inquiries and lawsuits. *The Wall Street Journal's* ongoing "[What They Know](#)" series, among other media exposés, has helped generate some of this unwanted attention for a number of parties in the mobile device, app and marketing sectors, including [Apple](#), [Google](#) and [Pandora](#).

While it will take years for regulators and case law to solidify the legal boundaries around any emerging technology, including mobile apps, businesses and marketers who want to avoid predictable legal scrutiny can reduce their risks now by adhering to traditional best practices around advertising and privacy.



Start With This Checklist

Don't Hide the Money Factor. If your app has a charge associated with it — whether as part of the initial purchase or within the app itself (e.g. purchase in-game content, accessories, etc.), disclose that point upfront using plain language in the description. Apply a “dummy” test — would your tech-challenged family member notice and read the disclosure, or is it buried under miles of terms and conditions?

Definitely Don't Hide the Money Factor if Your App is Targeted at Kids. If you expect that parents will be downloading your free app but kids will be playing it, consider whether in-game charges make sense from a business standpoint (weighed against the risks of parents claiming unauthorized charges by their children). If there is a sound business reason for the in-game charge options, make sure you clearly and conspicuously disclose the potential for charges up front in the description.

Assess Your Data Drilling. Unless you're closely watching courts and Congress, you might not have realized that mobile app user data comes with strings attached. You must assess exactly what user data your app is collecting (intentionally and unintentionally) and why it is doing so. Ask yourself these questions:

- Does this data collection involve name, contact details or other personally identifiable information on the user or their contacts?
- Does the app collect device location information and/or a unique identifier per user or device?
- Is there a necessary business reason for that data collection and access?
- Do you retain that data for a period of time consistent with the reason for collecting it?
- Do you share that data with other parties (or allow others to access that data), and can the parties use the data to make a personally identifiable profile of your users?

If you answered “yes” to any of the above, you should closely review how/if your app's terms communicate that to the user and whether users understand those terms and provide consent for such use.

Legalese Is Bad. If you plan to take care of everything identified above with a link to a lengthy boilerplate terms and conditions and privacy policy, think again. A legalese boilerplate won't insulate your business. The overriding question is whether you clearly communicated important terms — like charges and personal data practices — to the consumer in a way the consumer understood and accepted. That means ensuring that your app walks the user through these key terms in a just-in-time, user-friendly way.

*This article originally appeared on Mashable.com.
Published: May 26, 2011*



5 Privacy Tips for Location-Based Services

[Alysa Z. Hutnik](#) is a partner in the advertising law and privacy and information security practices at [Kelley Drye & Warren LLP](#). Her co-author, [Sharon K. Schiavetti](#), is an advertising and privacy associate at Kelley Drye & Warren LLP. Read more on Kelley Drye's advertising blog [Ad Law Access](#) or keep up with the group on [Facebook](#) or [Twitter](#).

The year 2012 is certain to reflect U.S. consumers' continued love affair with sophisticated smartphones and tablets. One of the driving forces in the popularity of these devices is their ability to run mobile apps using wireless location-based services (LBS). Among other benefits, LBS allow access to real-time and historical location information online – whether to facilitate a social interaction or event, play games, house-hunt or engage in many other activities.

However, with these benefits also come privacy risks. And it is not uncommon for some popular LBS-enabled tools to lack clear disclosure about personal information collection, how that data is used, and the process for consumer consent.

Failing to design a mobile app that covers these bases can be costly, inviting government investigations and lawsuits. For example, the U.S. Federal Trade Commission, which enforces consumer protection, has obtained 20-year [settlements](#) with numerous companies that engaged in deceptive or unfair practices by collecting personal information from consumers without appropriate disclosures or consent to such practices (including when personal information collection is set as a default). The commission has also targeted companies for engaging in practices that differ from their [privacy standards](#). Furthermore, class action lawsuits and [media scrutiny](#) regarding these types of practices continue to serve as warnings.

LBS-based businesses that want to avoid becoming future legal or media targets need to take stock of existing business practices and identify where updates may be appropriate. Take a look at the following privacy LBS do's and don'ts.

1. Privacy by Design

At a minimum, a business should know what its LBS service does, what type of data it collects, and whether that data is shared with affiliates, partners or third parties. Claiming ignorance to the data flow of consumer location information is not likely to protect a business from privacy-related liability.

Consider carefully the intentional and unintentional data flows from LBS offerings. Is the data personally identifiable, either individually or when combined with other elements, in the company's database? Will it be shared with an online advertiser, marketer or a social media platform like Facebook? Is there a legitimate business rationale for the collection, disclosure



and retention of such information? Understanding the data flows is the first step in preventing an LBS privacy mishap.

When performing such due diligence, businesses also should appoint privacy-trained personnel to ensure that privacy considerations are identified and satisfied, both at the outset of the design of a new service or product, as well as at periodic intervals after the service or product has been released publicly. These are the core principles of the FTC's "[privacy by design](#)" framework.

2. Transparency About LBS

Treat LBS information collection and disclosure as sensitive personal information, which means being transparent and careful with the data. This includes providing clear disclosures to consumers (before they download the LBS-enabled service) which explain:

- What personal information will be collected, retained and shared.
- The consumer's choices as to such data collection.
- How to exercise such choices.
- Provide a periodic reminder to consumers when their location information is being shared.
- If location information previously collected will be used for a new purpose, provide an updated disclosure to the consumer about the new use and an opportunity to exercise her choice as to that new use.

These disclosures should be presented prominently, in concise and plain language (i.e. not legalese or technical jargon).

3. User Consent

There can be some flexibility in how a business obtains a consumer's consent to LBS information. That being said, a business generally bears the burden of demonstrating that it obtained informed consent to the use or disclosure of location information before initiating an LBS service. Thus, it is *not* advisable to use pre-checked boxes or other default options that automatically opt users in to location information collection, or any other manner that ultimately leaves the consumer unaware of such data collection.

The key is to clearly provide a disclosure about the location information collection, to clearly obtain consumers' consent to use location information, and to keep accessible, organized business records of such disclosure and consent. It also is advisable to allow consumers the option of revoking consent previously given.



4. Treat Children's Data as Sensitive

The use of mobile devices by children and young adults raises additional privacy and safety concerns. Therefore, be sensitive to consumer expectations on how to treat such data, as well as to the extra legal scrutiny that accompanies marketing efforts targeted to young people. A business also needs to be mindful whether it is collecting location information from children under the age of 13, and the corresponding legal obligations that may be triggered under the federal children's privacy law (the Children's Online Privacy Protection Act). Navigating through these legal obligations with a privacy expert is critical to avoid mishaps.

5. Stay Current on Fast-Moving Privacy Developments

One common complaint by many a business is that it was unaware a particular business practice was considered unlawful (a complaint that is generally made after a regulator or litigant initiates legal action). A practical tip: In the sometimes murky area of consumer protection and privacy law, the rules of the road often are gleaned from analyzing cases, law enforcement examples and best practices, rather than from clear restrictions in a particular statute. For this reason, it makes good sense to periodically monitor law enforcement actions announced by the FTC and State Attorney General that highlight privacy-related practices, as well as guidelines issued by organizations that focus on LBS and privacy issues.

In 2012, we'll witness legal action against companies that engage in LBS without accounting for privacy developments. While privacy investment is not inexpensive, proactively implementing best privacy practices at the outset is far less costly than being singled out by regulators, litigants and the media after-the-fact.

BEST PRACTICES FOR MOBILE APPLICATIONS DEVELOPERS

SUMMARY

"Mobile applications" — the software programs written to execute on one or more mobile device operating systems (such as Android, Blackberry OS, iOS, Symbian or Windows Phone OS) – can collect and transfer end users' personal information from their mobile devices. Such transfer of personal information raises privacy issues. And privacy in mobile applications can be a challenge. Mobile platforms may have terms of use related to privacy but it is not always clear what those terms mean. Most developers are not experts in privacy law and policy and do not have the resources to hire lawyers or privacy consultants. The small screens of mobile devices limit the amount of information that can be easily communicated to users. Moreover, it may be difficult to understand how the third-party services incorporated into apps, such as analytics packages and those from advertising networks, use and access end users' information.

Although this document is aimed at app developers, we recognize that the ability to comply with leading practices described here may depend on other parties such as platforms, advertisers, ad networks and others. In some cases, providing the right notice and choice to the user may be best implemented by some of those other parties. Nonetheless, it is important to understand that as an app developer, you, rather than the platform or third-party services, have the most significant legal and ethical obligations to your users. Many countries place obligations on companies that collect, use, or transmit personal data. In the United States, the Federal Trade Commission has recently brought a number of enforcement actions against application developers accused of misusing user data. Nearly all app marketplaces require that you provide a written privacy notice if your app transmits data from the device.

One important thing to keep in mind is that many, if not most, privacy issues for application developers come from inserting third party code or software development kits(SDKs)—such as those from advertising networks or analytics providers—into your app. If you plug someone else's code into your application and then release it to a user without understanding how it collects, uses, or transmits your users' information, you are on the hook both legally and to users, with regard to the third parties you work with, and the analytics/practices they engage in. Make sure you understand what your third party providers are doing with user data, and make sure your users are informed and have control over how their information is used.

The following recommendations are based on the [Fair Information Practice Principles](#)— a set of generally accepted principles for how organizations should treat individuals' personal information. These principles include:

- Be completely transparent about how you are using or transmitting user data
- Don't access more data than you need, and get rid of old data
- Give your users control over uses of data that users might not expect
- Use reasonable and up-to-date security protocols to safeguard data

- As the app developer, you need to be responsible for thinking about privacy, and taking privacy into consideration during the various stages of your app life cycle

This document outlines best practices to guide you in building privacy into your application.

Transparency and Purpose Specification

- ***Have a Privacy Policy.***¹

The first step in respecting your users' privacy is to create a privacy policy that explains what you do with their data, and with whom you share it. This is an important process, even if you do not believe that you are collecting or using data that would trigger privacy concerns. The more information that you collect and use, the more detailed your privacy policy should be. Note that almost all applications collect information in some manner and for different purposes. If you are not actively collecting personal data, you are probably passively collecting personal data for authentication or similar purposes. If your app uses third party analytics or is ad supported, you are likely collecting or disclosing user information.

Do not just cut and paste a privacy policy from another app or website. Start by understanding *your* app in your own terms, and then do your best to communicate the same to your users. If you are using third-party code in your application, make sure you understand what those third parties are doing, and describe it clearly to your users. If you misstate what you are doing in your privacy policy (or elsewhere), you may bear legal responsibility for deceiving your users.

Companies like [PrivacyChoice](#) and [TRUSTe](#) provide excellent (and, to some extent, free) tools to help you create your own policies and short-form notices to your users. The [Mobile Marketing Association](#) has also put out a model privacy notice that can help guide the creation of your own policy. And the [Future of Privacy Forum](#) provides privacy resources for app developers at [ApplicationPrivacy.org](#).

Provide a link to your privacy policy in each app store listing and on your own site so that users can review it before downloading your app. Platforms and application stores should ensure that apps are able to provide a privacy link in advance. If your app has a settings page, place a privacy policy link there as well, and make sure that it leads to a page that can easily be read on a mobile device.

¹When developers sign up with a platform, they agree to the platform's terms of services. However, that is not a privacy policy that covers your relationship with your users.

EXAMPLES:



Apple: Developers must provide clear and complete information to users regarding collection, use and disclosure of user or device data. (Section 3.3.10 of the iOS Developer Program License Agreement)



Android: If users provide you with, or your app accesses or uses user names, passwords, or other log-in or personal information, you must make users aware that this information will be available to your app, and you must provide legally adequate privacy notice and protection for those users. (Section 4.3 of the [Android Market Developer Distribution Agreement](#))



Facebook: You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application. (Section II(3) of [Facebook Platform Policies](#))



Intel: If your application collects any personal information, the user must be notified about what is being collected, why it is being collected (purpose) and whether the information will be shared with anyone else (Section 1.1 of [Intel's AppUp\(SM\) developer program Privacy Requirements and Recommendations](#))



Microsoft: If your app shares a user's personal information (including, but not limited to Contacts, Photos, Phone number, SMS, Browsing history or unique device or user IDs combined with user information) with third parties, the application must implement a method to obtain "opt-in" consent. (Section 2.8 of the Certification Requirements)

- *Make extra effort to disclose and communicate unexpected uses of user data.*

A privacy policy is an important resource to help users, advocates and regulators understand your practices, but it is not the only place you should provide information about data collection and use.

If your app makes use of data in a way that users might not expect, you should make clear, conspicuous and timely disclosures of that fact.

Depending on the type of app, some unanticipated uses might include the following:

- Sharing data with an ad network for behavioral advertising use
- Working with third parties to allow other transactional data to be appended and used across sites
- Accessing or sharing precise geo-location sensitive information
- Accessing contacts

- Accessing other sensors or features on the phone (like a camera or microphone)
- Resetting a user's browser homepage
- Installing toolbars
- Changing default search

In many cases, it may be obvious to the user why you are collecting data. For example, if your app provides local restaurant reviews and asks a user for permission to access their current location, that purpose is obvious. However, if your app also transmits location information to third-party advertisers, that may not be obvious to users. In that case, your notice might say, "We need your location information to select restaurants near to you, and also so that our advertising partners can show more relevant advertising based on your location."

Platforms and applications stores should consider steps they can take that would allow apps more opportunity to explain the reasons why certain types of data are required in the app download or authorization process.

Even if user data is not tied to a real name (traditionally called "personally identifiable information," or "PII"), you should still inform users if the data is linkable back to a particular record or device. People have a privacy interest in "pseudonymous" or "anonymous" data if that data is used to customize or alter the user's experience, or if it could reasonably be linked back to the individual through reidentification or through a government subpoena (or other legal means).

- ***Share new data use policies before implementing them to give your users notice and time to understand them.***

Whenever you update your app, review your privacy policy to confirm that it accurately describes your current data practices. If you change your data practices, give your users advance notice. For example, posting an updated privacy policy 30 days in advance will give your users time to digest the changes and notify you of any questions or concerns. If your updated policy includes a new, unexpected usage of any data (including pseudonymous data), especially unexpected transfers of information to third parties, you should be especially clear and conspicuous in your notice. When you post a new policy, tell your users upfront what has changed, so they do not have to parse through the old and new policy to see what is different.

A simple way to notify users of privacy policy changes is to include the date of the most recent update in the anchor text of your policy link, such as "Our privacy policy (updated 10-28-11)."

Use Policies and Limitations

- ***Be clear and specific in your disclosures.***

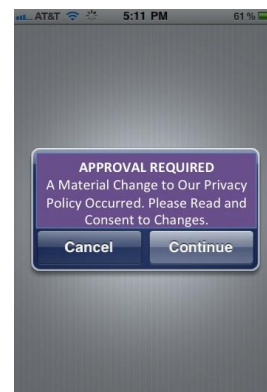
When you issue your privacy policy, be specific when you list uses of user data. Do not be ambiguous or try and reserve all rights to the data. To the extent that it is practical, also disclose the exact third parties (if any) with whom you share your users' data. If nothing else, you should clearly identify the *types* of companies with which you share user data. If you cannot clearly articulate to users a reason why you are collecting certain data, do not collect it.

- ***Stay within the boundaries of your disclosures; don't use or collect data if you haven't explained the practice to the user.***

If you have not explained a particular use of your users' data in your privacy policy (or elsewhere), do not use the data in that way. Undisclosed data practices can get you into trouble with the FTC or other regulators. Obviously, you may not be able to envision every possible use of user data when you write a policy, but try to keep your policies up-to-date as your data usage practices change.


- ***If you make material changes to your data policies and practices, get new permission from your users before using old data.***

If you make a material change or update to your data use policies, you should obtain affirmative, opt-in consent from your users before using previously collected data in new ways. In the U.S., the FTC and State Attorneys General have brought enforcement actions against companies that tried to retroactively change privacy policies to allow for new data uses. (And do not rely on language in a privacy policy that reserves the right to change the policy at any time — courts have found those to be unfair and invalid.)



- ***Don't access or collect user data unless your app requires it.***

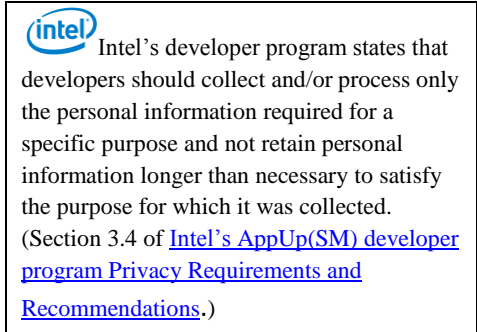
Don't take what you don't need. If you gather or transmit data that your app does not need for a legitimate purpose, you put both yourself and your users at risk. Advertising may well be a legitimate purpose—so long as the collection and transfer of targeting data is transparent, and users are given options about usage of their information for that purpose (see “Individual Choice,” below). However, platform and app stores may have their own rules about the collection and use of user information for certain purposes, including advertising. Violating a platform's terms of service could get you in trouble with the platform or app store, or with regulators who assert

 Apple obtains information about the device's precise location (the latitude/longitude coordinates) when an ad request is made. However, Apple immediately converts the precise location data to the five-digit zip code, and then discards the coordinates. Apple does not record or store the precise location information, only the zip code. ([Apple letter to Rep. Markey on location, May 2011.](#))

that a platform or app stores' rules create reasonable expectations on the part of the user about how their information will be treated. Delete data that does not need to be retained for a clear business purpose.

- **Delete old data.**

Get rid of user data that you don't need anymore. Don't just keep user data around indefinitely on the off-chance that it may be valuable some day. This applies whether you store user data on the device, or your own servers, or in a cloud platform. Remember to clear associated metadata or cross-references to deleted data. These practices respect your users' privacy interests and helps protect you and users in the event of a data breach (if your security is breached, you may be legally responsible for failing to exercise reasonable security procedures, and for informing users that their data has been compromised). In lieu of deletion, deidentification of the data may be sufficient if there is no reasonable chance the data could be linked back to an individual or device. Consider the retention periods of your vendors as well when assessing any third-party service to which you will be sending user data.

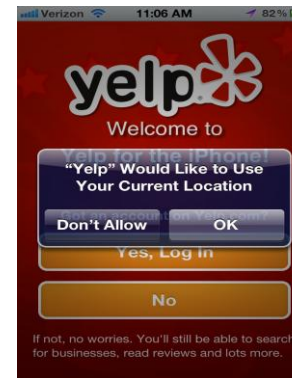


You should also delete user data promptly following the deletion of an account. Users should rightly expect that once they close their account, all data be deleted from your server.

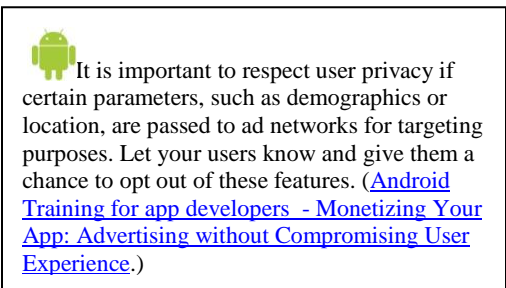
Individual Choice

- **Provide stronger protections and enhanced control over sensitive information.**

Sensitive information about your users warrants stronger protections. The definition of "sensitive" may vary from jurisdiction to jurisdiction, but often includes data related to health, finances, race, religion, political affiliation or party membership, and sexuality. If your app collects or transmits data associated with any of these categories, you should make an extra effort to ensure your user understands this and expressly agrees to its use. Simply describing these uses in a privacy policy or terms of use is not sufficient.



Precise geo-location information is increasingly considered sensitive information as well, and you should only collect and transmit such information when you have your users' clear, opt-in permission. While most platforms do require express permission for an app to access location information, if you are using that data in unexpected ways or transmitting that



information to third-parties, make sure you get your own permission from the user before doing so.

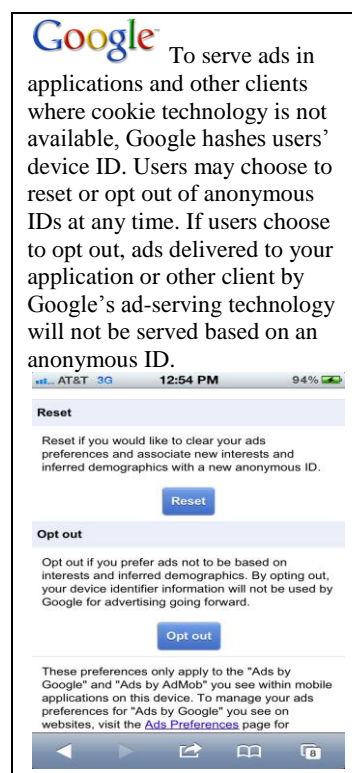
- ***Give users choice around the unexpected collection, storage, or transfer of personal information.***

You should give users meaningful control over their information. If you are collecting or using data outside the scope of what users would reasonably expect, you should at the very least make sure your users can opt-out of such uses of their data. When a user opts-out, you should stop sending personal data to third-party advertising partners (or stop letting third parties access user data from the device or elsewhere) or make sure they have procedures in place to not track users across applications. If your advertising partners offer users the ability to persistently opt-out of the tracking and usage of their data, you can rely on these opt-outs so long as you conspicuously describe and link to those opt-outs in your own policies and disclosures (at least in the United States).

If you are accepting ads provided by a third-party ad network, it is quite possible that user data is being used to tailor ads on other apps or that you are passing along unique, fixed device identifiers to that ad network. You should only work with third parties that either do not engage in such targeting or give users choice around such targeting. Your privacy policy should clearly explain that you are sharing behavioral and device identifier information with third parties (when applicable), identify those third parties, and link to information about how to opt-out of such tracking or targeting. You should also consider whether you can provide your own functionality to allow users to prohibit transfer to a third party of a unique tracking identifier.

For example, the [Digital Advertising Alliance \(DAA\) principles](#) are one method of providing notice and choice of advertising options. We recognize that the current tracking and user control options available to apps are limited by platform technologies and policies. Cookies are unavailable, as are cookie controls or other tracking control options. Platforms should consider providing users with privacy controls that can be used to block or manage the tracking mechanisms used by third parties. For example, iOS5 provides users the opportunity to opt-out of sharing location with iAds and Android provides users with the opportunity to decline behavioral advertising with Google's AdMob division. Platforms should similarly provide options or APIs that would enable other third parties with similar options to provide users with a choice to opt-out of being tracked or profiled.

You do not, however, have to offer choice around all uses or transfers of data. If the collection and use of the data is obvious and related to the product you offer, it can be assumed that the user has consented to these uses (you should still make sure you describe these uses in your privacy



policy). The Federal Trade Commission has recently stated that for “commonly accepted” data usages, such as product fulfillment, first-party analytics, security, and accounting and back-office operations, companies should not have to offer users control around such data uses. In some jurisdictions, regulators may require consent for anything other than purposes that are essential for the operation of the app.


In some jurisdictions, notably the European Union, regulators have called for the provision of express consent in certain circumstances, such as when tracking cookies or other unique identifiers are used for behavioral advertising. If you provide your app to European users, you should carefully follow developments in this area.

- ***If you condition use of your app on the collection and use personal information, educate your users about the trade-off.***

If you want to condition distribution of your app on certain data usage — such as sharing personal information with ad networks — that’s fine. If your application is a “take it or leave it” deal, make a clear value proposition to your users so they understand the exchange. Many users may be happy to share their personal information in exchange for your app. However, you need to be clear and up front in your explanation. Also, note that while CDT and FPF think it may be appropriate for apps in a robust marketplace to require consent to “tracking” in exchange for offering users a service, this practice may soon be prohibited in Europe under recently proposed legislation.

- ***If feasible, let your users have access to the data you keep about them or their device.***

If you are keeping records on your users in the normal course of business, you should try to set up a mechanism so that users can readily see what information you are collecting and storing about them. If you are transmitting data to third parties, such as ad networks, you should try to select partners that also offer users reasonable access to the files created about them. Granting access to such data is legally required in many jurisdictions, such as the European Union. It doesn’t matter whether you live in Europe or not — if you collect information from European users, you may well have the legal obligation to make the information you collect and use available to users.

 You should provide individuals reasonable access to their personal information so the individual can ensure their personal information is accurate, complete and current (Section 3.3 of [Intel’s AppUp\(SM\) developer program Privacy Requirements and Recommendations](#)).

Also, you should strive to ensure that the user personal information you collect, store, and transfer is as accurate, complete, and up-to-date as is needed for the specific use by the app.

Security

- ***Understand the risks associated with your app, and ensure appropriate and reasonable security measures are in place.***

Understand the security risks associated with your app such as the sensitivity of information you collect and store, and the number of users using the app. All applications that access, use, or transfer individuals' data should be tested rigorously for security purposes. However, all apps should comply with current and reasonable best practices for security.

- ***Encrypt data in transit (e.g., using SSL/TLS) when authenticating users or transferring personal information.***

Your app should provide appropriate protections for user data in-transit, especially when that data is authentication data, session data, or personal information. New hacking tools have made snooping on unsecure connections quite simple, especially on unsecured Wi-Fi networks. You can avoid many of these problems by using SSL/TLS for all communications with your server, as modern back-end providers should have little problem scaling SSL even to a large number of transactions.

- ***Encrypt data you store about or on behalf of your users, especially sensitive information and passwords.***

Whenever feasible, you should ensure you are encrypting your users' data, especially authentication information like usernames, email addresses, and passwords. Storing unencrypted data puts both you and your users at risk in the event of a data breach.

- ***Protect user application data.***

Make sure users can log out of a session using the mobile client, and that password changes on the back-end side invalidate mobile clients' current sessions. If your application accesses, collects, or stores sensitive data or is a fruitful target for phishing attacks, consider using two-factor authentication such as confirmation text messages, or one-time application-specific passwords.

Accountability

- ***Make sure someone is responsible for privacy.***

You should have at least one person responsible for making sure that privacy protections are integrated into your product. If you are a one-man shop, then this is your job. This means that:

- You **review your privacy policy** before each app release, to ensure that it remains accurate and complete,

- You **keep an archive** of your privacy policy, and ensure that change notices are appropriately posted for users,
- You **confirm your company's rules** for who can access data internally, to ensure that personal information is only available to team members with a need to see it,
- You **answer all privacy-related emails** and communication, and
- You **remain on top of new developments** by following the FTC and other industry organizations.

- ***Practice Privacy by Design.***

Privacy should ultimately become a consideration central to your design process and considered at all stages of app development. Responsible app development goes above and beyond compliance with regulatory requirements and law; strive to make privacy assurance a default mode of operation. Take privacy into consideration during all phases of the life cycle of your application.

- ***Provide users with a way to contact you and respond to questions and concerns.***

Provide your users with the opportunity to contact you with questions, concerns, or complaints. This can be accomplished through a simple form accessible from within your app, an email address where your users can contact you, or a feedback forum. Consider highlighting common privacy and security topics. Take the time to review and respond to your users' messages; don't merely provide a means for feedback and then fail to follow up. Good communication is good for privacy and your business.

Special Considerations

- ***Make sure you comply with applicable laws and regulations.***

In the United States, there is a patchwork of federal and state laws protecting certain kinds of information. Most app developers do not work with user data explicitly governed by a federal law. However, federal laws and regulations do extend to user credit reports, electronic communications, education records, bank records, video rental records, health information, children's information and user financial information. If your app handles information in these areas, you should consult with an attorney or privacy expert.

You should consider the sampling of federal privacy laws and regulatory agencies listed below. If you think you might be covered, conduct further research and/or seek out some legal advice. By providing an application, you are responsible for compliance with all applicable laws.

- ***Fair Credit Reporting Act of 1970 (FCRA)***
Sets forth responsibilities for "credit reporting agencies," and entities that provide credit report agencies with data, regarding the preparation and dissemination of personal information in user reports for credit, employment, and other important eligibility purposes.

- *Health Insurance Portability and Accountability Act of 1996 (HIPPA)*
Sets forth national privacy standards for the protection of individually identifiable health information for certain regulated entities.
- *Children's Online Privacy Protection Act of 1998 (COPPA)*
Sets forth rules governing the online collection of information from children under 13 years of age, including restrictions on marketing to those under 13 years of age (see below for more information).
- *CAN-SPAM Act of 2003*
Sets forth rules for the sending of commercial e-mail requiring visible and operable unsubscribe mechanisms, accurate subject lines, and other user protections.
- *Video Privacy Protection Act (VPPA)*
Sets forth rules generally banning the disclosure of personally-identifiable rental or sales records of audiovisual materials (absent written consent).
- *Gramm–Leach–Bliley Act (GLB), aka Financial Services Modernization Act of 1999*
Sets forth rules for financial institutions requiring disclosure of privacy policies and user opt-outs for the sharing of personal information.
- *Federal Trade Commission “Unfair and Deceptive” Authority*
The Federal Trade Commission (FTC) has general authority to police “unfair or deceptive acts affecting commerce.” The FTC frequently confronts online services that are unclear or deceptive in their collection and use of personal information.

In Europe, the legal framework consists of national laws and legislation (e.g. Directives) of the European Union — in some countries there will even be different state law on privacy. This is matched by a number of different agencies with different enforcement mechanisms. The main difference from the United States approach is that *all* data is governed by legal requirements, instead of the relatively narrow sector-specific categories described above.

- *Directive 95/46 of the European Parliament and of the Council of 24 of October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of the data*

Relevant passages include the obligation to have technical and organizational measures to prevent data leakage (Art. 17); information duties (Art. 10-11) and access rights (Art. 12) and rules on international data transfers (Art. 25 ff.)

- *Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*

Relevant passages include security (Art. 4); confidentiality of communication including the consent requirement for placing information on terminal equipment (Art. 5) and use of location data (Art. 9).

- *Information Commissioner's office (ICO), United Kingdom*

While only one of many data protection authorities in Europe, the ICO has comprehensive information about European data protection law. The UK's guidance is especially relevant because of the new power to fine organizations up to \$800,000.

- ***Special considerations for children and teenagers.***

If your app is directed at an audience of children 12 and under, it's likely that you will have to comply with the Children's Online Privacy Protection Act (COPPA). COPPA requires you to obtain "verifiable parental consent" before collecting any personal information -- including name, email address, or phone number -- from a child. So if your app is tailored for young kids, be sure not to request that kind of information unless you have a parent's consent first. (There are specific regulatory guidelines that lay out your options for obtaining verifiable parental consent; you should consult with an expert before attempting to collect personal information from children.)

In general, it's a good idea to treat kids' and teens' data very sensitively. The Federal Trade Commission is actively reviewing COPPA's scope and how it applies to app developers, and youth online privacy is a hot-button issue with legislators, regulators, and the press. Any app that seeks out minors will likely face a lot of scrutiny, so keep your data collection to an absolute minimum. You should avoid sharing kids' or teens' information with third parties and should provide clear, age-appropriate notice about any data you do collect or share.

If your app is aimed at kids, you should not share information with ad networks for the purpose of behavioral advertising or any other party (such as mobile analytics companies).

- ***Stay informed of new developments (like "Do Not Track").***

New privacy rules and policies are developing quickly. As a developer, you should stay abreast of these developments.

For example, the FTC recently recommended a "Do Not Track" regime that would make it easy for users to universally opt-out of tracking across websites online. Major Internet browsers have already implemented "Do Not Track" controls, and many are advocating for similar tools on mobile devices. If mobile operating systems begin to deploy "Do Not Track"-type settings, you should consider how to implement those controls and how your third-party partners respect such controls in order to align with your users' reasonable expectations.

Additional Resources

[Future of Privacy Forum Application Privacy Site](#)

[PrivacyChoice Mobile Resources](#)

[TRUSTe Mobile Privacy Solutions](#)

[Mobile Marketing Association](#)

[IPC Ontario Privacy By Design](#)



**Best Practices and Guidelines
for
Location-Based Services**

Version 2.0

Effective Date: March 23, 2010

CTIA’s Best Practices and Guidelines for Location Based Services

TABLE OF CONTENTS

Section 1 - Purpose	1
Section 2 – Applicability	1
Section 3 – Scope of Coverage	2
Section 4 - Specific Guidelines.....	3
A. Notice	3
B. Consent.....	5
1. Form of Consent	5
2. Account Holder Consent.....	5
3. Revocation of Consent.....	6
C. Safeguards	7
1. Security of Location Information.....	7
2. Retention and Storage of Location Information	7
3. Reporting Abuse	7
4. Compliance with Laws	7
5. Education	7
6. Innovation	8
7. Compliance with Guidelines.....	8
Appendix – Additional References:.....	8

** The examples provided in the Guidelines are illustrative only and are not meant to indicate that LBS Providers must provide the features or services described in the examples.*

Section 1 - Purpose

CTIA Best Practices and Guidelines (“Guidelines”) are intended to promote and protect user privacy as new and exciting Location-Based Services (“LBS”) are developed and deployed. Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. Accordingly, the Guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.).

The Guidelines primarily focus on the user whose location information is used or disclosed. It is the user whose privacy is most at risk if location information is misused or disclosed without authorization or knowledge. Because there are many potential participants who play some role in delivery of LBS to users (e.g., an application creator/provider, an aggregator of location information, a carrier providing network location information, etc.), the Guidelines adopt a user perspective to clearly identify which entity in the LBS value chain is obligated to comply with the Guidelines. Throughout the Guidelines, that entity is referred to as the LBS Provider.

The Guidelines rely on two fundamental principles: user notice and consent.

- First, LBS Providers must ensure that users receive meaningful notice about how location information will be used, disclosed and protected so that users can make informed decisions whether or not to use the LBS and thus will have control over their location information.
- Second, LBS Providers must ensure that users consent to the use or disclosure of location information, and LBS Providers bear the burden of demonstrating such consent. Users must have the right to revoke consent or terminate the LBS at any time.

Users should have confidence when obtaining an LBS from those LBS Providers that have adopted the Guidelines that their location information will be protected and used or disclosed only as described in LBS Provider notices. By receiving notice and providing consent consistent with these Guidelines, users will maintain control over their location information. The Guidelines encourage LBS Providers to develop and deploy new technology to empower users to exercise control over their location information and to find ways to deliver effective notice and obtain consent regardless of the device or technology used or business model employed.

Section 2 – Applicability

The Guidelines apply to LBS Providers. The following examples identify common situations and illustrate who is and is not an LBS Provider with obligations under the Guidelines.

Examples of LBS Providers:

Example 1. *A wireless carrier is the LBS Provider when it directly provides account holders or users an enhanced 411 LBS to locate nearby businesses.*

Example 2. *An application developer that provides the service for a downloadable LBS application (e.g., turn-by-turn driving) that is offered through an application storefront is the LBS Provider; a wireless carrier that provides user location information to that application developer for use in the LBS (e.g., through incidental assistance to the device's A-GPS or through other network data) is not an LBS Provider.*

Example 3. *A device manufacturer that pre-loads its own manufacturer-branded LBS application (e.g., a proprietary social networking application) is the LBS Provider; a device manufacturer that merely includes location enabled technology (e.g., A-GPS) on the device to support other applications and services, is not an LBS Provider.*

Example 4. *An entity that merely enables application providers to access location information from multiple wireless carriers (i.e., an aggregator) is not an LBS Provider, nor are the wireless carriers LBS Providers; instead, a party that uses an aggregator's data to make an LBS available to users is the LBS Provider.*

Example 5. *A wireless carrier that provides its customers "on-deck" access to a mapping service provided by a separate software developer is not the LBS Provider even if it provides the location information used by the third party; instead, the software developer is the LBS Provider.*

Caveat: The examples are illustrative only and do not imply that compliance with the Guidelines alone permits such uses or services. The terms on which access to location information is made available from wireless carriers to third parties, or the terms under which applications are made available to users, are beyond the scope of the Guidelines.

Section 3 – Scope of Coverage

The Guidelines apply whenever location information is linked by the LBS Provider to a specific device (e.g., linked by phone number, userID) or a specific person (e.g., linked by name or other unique identifier).

The Guidelines do not apply to location information used or disclosed:

- as authorized or required by applicable law (e.g., to respond to emergencies, E911, or legal process);
- to protect the rights and property of LBS Providers, users or other providers of location information;
- for testing or maintenance in the normal operation of any network or LBS; or
- in the form of aggregate or anonymous data.

Section 4 - Specific Guidelines

A. Notice

An important element of the Guidelines is *notice*. LBS Providers must ensure that potential users are informed about how their location information will be used, disclosed and protected so that they can make informed decisions whether or not to use the LBS, giving the user ultimate control over their location information.

The Guidelines do not dictate the form, placement, terminology used or manner of delivery of notices. LBS Providers may use written, electronic or oral notice so long as users have an opportunity to be fully informed of LBS Providers' information practices. Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous.

If, after having obtained consent, LBS Providers want to use location information for a new or materially different purpose not disclosed in the original notice, they must provide users with further notice and obtain consent to the new or other use.

LBS Providers must inform users how long any location information will be retained, if at all. If it is not practicable to provide an exact retention period, because, for example, the retention period depends on particular circumstances, the LBS Provider may explain that to users when disclosing its retention policies.

LBS Providers that use location information to create aggregate or anonymous data by removing or permanently obscuring information that identifies a specific device or user must nevertheless provide notice of the use.

Example 6. *An LBS Provider could create a dataset of mobile Internet users registered in a particular geographic or coverage area by removing or "hashing" information that identifies individual users from the dataset so that the LBS Provider could provide location-sensitive traffic management information or content to a highway safety organization. Notice that the LBS Provider creates or uses aggregate or anonymous data is required.*

LBS Providers that share location information with third parties must disclose what information will be provided and to what types of third parties so that users can understand what risks may be associated with such disclosures.

LBS Providers must inform users how they may terminate the LBS, and the implications of doing so. LBS Providers also must ensure that any privacy options or controls available to users to restrict use or disclosure of location information by or to others are explained to users.

Example 7. *An LBS Provider that offers a social networking service might provide a mechanism for the user to establish permissions for when, where and to whom his or her location information will be disclosed. The notice to the user could include a statement to the effect:*

“You control who will receive your location information. In ‘settings’ on the menu, you can select contacts you wish to block or enable all the time, or you can select a manual option to review a list of contacts each time you disclose your location.”

LBS Providers must periodically remind users when their location information may be shared with others and of the users’ location privacy options, if any. The form, placement, terminology used, manner of delivery, timing and frequency of such notice depends on the nature of the LBS. For example, one would expect more reminders when the service involves frequent sharing of location information with third parties and fewer reminders, if any, when the service involves one-time, user-initiated concierge service calls (e.g., locating a nearby service). In addition, depending on the circumstances, the use of an icon or other symbol to disclose when location information may be shared may be a more effective means of reminding consumers than a written notice.

In some circumstances, account holders (as opposed to users) may control the installation and operation of LBS. In addition to providing notice to the account holder, LBS Providers still must ensure that notice is provided to each user or device that location information is being used by or disclosed to the account holder or others. Once again, the content, timing and frequency of such notice depends on the nature of the LBS.

Example 8. *An LBS Provider provides an LBS to a business customer with multiple devices used by employees in the field. The LBS Provider could satisfy its notice obligation by direct notice to each device that location information is being provided to the business customer. Alternatively, pursuant to a contractual obligation between the LBS Provider and the business customer to do so, the business customer could inform its employees that it will receive user location information.*

B. Consent

1. Form of Consent

LBS Providers must obtain user consent to the use or disclosure of location information before initiating an LBS (except in the circumstances described below where consent is obtained from account holders and users are informed of such use or disclosure). The form of consent may vary with the type of service or other circumstances, but LBS Providers bear the burden of establishing that consent to the use or disclosure of location information has been obtained before initiating an LBS.

The Guidelines do not dictate the form, placement, terminology used, or manner of obtaining consent as long as the consent is informed and based on notice consistent with the requirements set forth in the Notice section above. Consent may be implicit, such as when users request a service that obviously relies on the location of their device. Notice may be contained in the terms and conditions of service for an LBS to which users subscribe. Users may manifest consent to those terms and conditions electronically by clicking "I accept"; verbally by authorizing the disclosure to a customer service representative; through an IVR system or any other system reasonably calculated to confirm consent. Pre-checked boxes that automatically opt users in to location information disclosure, or, choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent.

2. Account Holder Consent

In some cases, where the actual user is different than the account holder, an account holder may control the installation and operation of LBS (e.g., business account holder utilizing LBS for fleet management; parental account holder providing phones for childrens' use). Under these circumstances, the appropriate consent may be obtained solely from the account holder. As noted above, however, LBS Providers still must ensure that notice is provided to each user or device that location information is being used by or disclosed to the account holder or others.

The following examples are illustrative of account holder consent upon which the LBS Provider may rely to use or disclose users' location:

Example 9. *Fleet Tracking/Employee Monitoring: A business entity purchases multiple lines to permit tracking employee locations to provide for rapid response repair service, just-in-time delivery, or fleet management.*

Example 10. *Public Safety: The LBS Provider enters into an agreement with a public safety organization to provide monitoring compliance with terms of supervised release and house arrest, terms of bail for bondsmen, protecting public officials on duty, or military force movements.*

Example 11. *Parental Controls: The LBS Provider offers a service to notify parents when a child arrives at or leaves a designated place.*

Example 12. *Family Safety: The LBS Provider offers a family safety feature to locate family members in an emergency or other specified circumstances.*

3. Revocation of Consent

LBS Providers must allow users to revoke their prior consent to use or disclose location information to all or specified groups or persons.

Example 13. *User signs up with an LBS Provider for a service that provides updates regarding user's location to a group of "friends" designated by the user. The LBS Provider must provide reasonable mechanisms for the user to discontinue such location sharing with the group at a later date.*

Where technically feasible, LBS Providers may provide for selective termination or restriction of an LBS upon account holder request. An account holder may revoke or terminate all or a portion of any users' consent to an LBS.

Example 14. *User signs up with an LBS Provider for a service that requires user's wireless carrier to periodically disclose user's location information to LBS Provider. User is a minor and the mobile device is one of several on the account of the wireless carrier's account holder who, through controls provided by the LBS Provider or upon request to the LBS Provider, decides to block the LBS or disclosure of user's location information to third parties. The account holder's election with the LBS Provider revokes the user's consent.*

Similarly, revocation of consent also occurs when certain controls for sharing location information are provided by a wireless carrier, and the account holder of the wireless carrier has decided to block disclosure of a user's location information to third parties for a line on the account holder's account.

The Guidelines do not dictate terms of service that LBS Providers must offer to users with regard to an LBS. Nor do the Guidelines dictate any technical implementation for terminating or restricting an LBS.

C. Safeguards

1. Security of Location Information

LBS Providers must employ reasonable administrative, physical and/or technical safeguards to protect a user's location information from unauthorized access, alteration, destruction, use or disclosure. LBS Providers should use contractual measures when appropriate to protect the security, integrity and privacy of user location information.

2. Retention and Storage of Location Information

LBS Providers should retain user location information only as long as business needs require, and then must destroy or render unreadable such information on disposal. If it is necessary to retain location information for long-term use, where feasible, LBS Providers should convert location information to aggregate or anonymized data.

3. Reporting Abuse

LBS Providers should provide a resource for users to report abuse and provide a process that can address that abuse in a timely manner.

4. Compliance with Laws

LBS Providers must comply with applicable laws regarding the use and disclosure of location information, and in particular, laws regarding the protection of minors. In addition, it is recommended that LBS Providers comply with applicable industry best practices and model codes.

5. Education

In addition to any notices required under the Guidelines, LBS Providers certifying under the Guidelines will work with CTIA in an education campaign to inform users regarding the responsible use of LBS and the privacy and other risks associated with the disclosure of location information to unauthorized or unknown third parties. All entities involved in the delivery of LBS, including wireless carriers, device manufacturers, operating system developers, application aggregators and storefront providers, should work to educate users about the location capabilities of the devices, systems, and applications they use as well as to inform them of the various privacy protections available.

6. Innovation

LBS Providers develop and deploy technology to empower users to exercise control over their location information and to find ways to deliver effective notice and obtain consent regardless of the device or technology used or business model employed.

7. Compliance with Guidelines

LBS Providers that comply with the Guidelines may self-certify such compliance by placing the following statement in their marketing or promotional materials:

LBS Provider follows CTIA's Best Practices and Guidelines for Location-Based Services.

Appendix – Additional References

CTIA has collected a variety of Location Based Services Privacy Policies that demonstrate the application of these Best Practices. These policies are available at:

http://www.ctia.org/business_resources/wic/index.cfm/AID/11924

Gonzalo E. Mon
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
202.342.8576
gmon@kelleydrye.com

John J. Heitmann
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
202.342.8544
jheitmann@kelleydrye.com

Christopher M. Loeffler
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
202.342.8429
cloeffler@kelleydrye.com

The following outline provides a summary of key issues to consider when developing and using location-based applications (“apps”) for mobile devices. Each situation is unique and the legal landscape is still developing, however, so you should consult an attorney before launching a location-based app.

I. OVERVIEW

A. TRENDS IN SMARTPHONE AND APP USE

1. The adoption rate for smartphones and use of apps continues to grow. A recent study indicates that nearly one quarter of U.S. adults have dropped their landlines and only use a mobile phone. Additionally, 35% of the adult population has mobile phones with apps installed on them.¹
2. The app market will continue to be attractive to device manufacturers and developers. Forecasted mobile app revenue for the four major app stores² is forecasted at \$3.8 billion for 2011.³
3. Apps including location-based technology continue to be popular options. These can include apps that let people identify their location and share information with friends through social networking platforms, to apps that help people find stores, restaurants, or points of interest near them, to instant location-based coupons.

B. DEVELOPING LEGAL LANDSCAPE

1. The legal landscape surrounding location-based apps is still developing. Legislators, regulators, privacy advocates, and industry participants continue to develop the parameters of what will be permissible practices.

¹ Kristen Purcell, Roger Entner, Nichole Henderson, *The Rise of Apps Culture*, Pew Internet (Sept. 14, 2010), available at http://pewinternet.org/~media/Files/Reports/2010/PIP_Nielsen%20Apps%20Report.pdf.

² Apple, Google, Nokia, and Research in Motion (RIM).

³ IHS Screen Digest Research, *Revenue for Major Mobile App Stores to Rise 77.7% in 2011*, <http://www.isuppli.com/media-research/news/pages/revenue-for-major-mobile-app-stores-to-rise-77-7-percent-in-2011.aspx> (May 3, 2011).

2. Recent scrutiny on mobile apps, particularly regarding location-based apps that permit device tracking has come in several forms: (a) investigative reporting; (b) Congressional inquiries and investigations; (c) regularly agency and administrative investigations by the Federal Trade Commission (“FTC”), Federal Communications Commission (“FCC”), Federal prosecutors, and state Attorneys General; and (d) class action lawsuits.
3. Unless and until legislation or more defined regulatory requirements are enacted, participants in the location-based app market should follow best practices that are grounded in legislative proposals and takeaways from Congressional hearings, regulatory enforcement actions and policy statements, guidance based on consumer concerns raised in private litigation, and industry sector recommendations.

II. INVESTIGATIVE REPORTING

A. SCOPE OF REPORTING

1. Investigative reporting in renowned publications such as the *Washington Post*, *Wall Street Journal*, and *New York Times* focused on data collection and location tracking functionality unknown to users, thus raising privacy concerns.⁴
2. Various reports indicated that Apple iPhone and Google Android phones collect location-based information from user’s phones and transmit that information back to the corporations. Transmissions are tied to a unique identifier tied to each particular phone.⁵

B. CATALYST FOR FURTHER INQUIRY AND CLASS ACTIONS

1. Investigative reporting has been a catalyst for Congressional inquiries and investigations, as well as private class action complaints against device and operating system manufacturers and application developers.
2. At least nine public letters or inquiries from regulators were issued to industry participants ranging from device and operating system manufacturers to wireless carriers. An unknown number of nonpublic letters or inquiries have been issued.

⁴ See, e.g., Wall Street Journal, *What They Know* Series, <http://online.wsj.com/public/page/what-they-know-digital-privacy.html>.

⁵ See, e.g., Julia Angwin and Jennifer Valentino-Devries, *Apple, Google Collect User Data*, Wall Street Journal (Apr. 22, 2011), available at <http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html>; Miguel Helft and Kevin J. O’Brien, *Inquiries Grow Over Apple’s Data Collection Practices*, N.Y. Times (Apr. 21, 2011), available at <http://www.nytimes.com/2011/04/22/technology/22data.html>; Miguel Helft, *Google Says It Collects Location Data on Phones for Location Services*, N.Y. Times (Apr. 22, 2011), available at

3. More than ten class action complaints were filed shortly after the investigative reports were released and Congressional and regulatory inquiries began.⁶

III. LEGISLATIVE ACTIVITY

A. LEGISLATIVE INQUIRIES AND HEARINGS

1. Beginning in approximately March 2011, Congressional Committees and members began issuing a flurry of letters and requested mobile industry members to respond to inquiries and participate in hearings.
2. On March 29, 2011, Reps. Markey (D-MA) and Barton (R-TX) send letters to Sprint, T-Mobile, Verizon, and AT&T asking about collection and storage of user location data. These letters were sent in response to a *New York Times* story regarding Deutsche Telekom's ability to track the locations of German politicians.⁷
3. On April 20, 2011, Sen. Franken (D-MN) sends a letter to Apple seeking more information on iPhone and iPad location tracking.⁸
4. On April 21, 2011, Rep. Markey (D-MA) sends a letter to Apple seeking information on the company's device location-tracking practices.⁹
5. On April 25, 2011, the House Energy & Commerce Committee sent letters to Apple, Google, Microsoft, Nokia, Research in Motion, and Hewlett Packard concerning device location-tracking practices.¹⁰
6. On May 10, 2011, the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law used its "first-ever hearing to examine whether federal laws protecting consumer privacy-particularly when it comes to mobile devices-are keeping pace with technological advances. Recent reports that Apple and Google operating systems track unwitting users' locations spurred widespread concern across the nation about how the information could be used."¹¹

⁶ Some class actions were consolidated.

⁷ Press Release, *March 30, 2011: Markey, Barton Ask U.S. Wireless Companies to Explain How They Track Their Customers* (Mar. 30, 2011), available at <http://markey.house.gov/index.php?option=content&task=view&id=4287&Itemid=125>.

⁸ Press Release, *Sen. Franken to Apple CEO: Apple's Operating System Raises Serious Privacy Concerns* (Apr. 20, 2011), available at http://www.franken.senate.gov/?p=press_release&id=1455.

⁹ Press Release, *April 21, 2011: Markey to Apple: Is it iPhone or iTrack?* (Apr. 21, 2011), available at http://markey.house.gov/index.php?option=com_content&task=view&id=4316&Itemid=141.

¹⁰ Press Release, *Letters to Mobile Device Operating System Developers* (Apr. 25, 2011), available at <http://energycommerce.house.gov/news/PRArticle.aspx?NewsID=8527>.

¹¹ Press Release, *Chairman Franken Presses Apple and Google to Protect Safety and Privacy of Mobile Device Users*, (May 10, 2011), available at http://www.franken.senate.gov/?p=press_release&id=1498.

B. PROPOSED LEGISLATION

1. While recent legislation in the 112th Congress has focused on data security and breach notice, several bills proposed in the early part of this session have included express provisions addressing mobile applications. These bills are still pending in the current session of Congress.
2. H.R. 611 – BEST PRACTICES Act, sponsored by Rep. Bobby Rush (D-IL), expressly includes a “mobile service” within the definition of a “third party” for data collection purposes. Additionally, “precise geolocation information and any information about the individual’s activities and relationships associated with such geolocation” is considered “sensitive information.”¹² The bill is designed to create transparency about the commercial use of personal information, and provide consumers with choice about the collection, use, and disclosure of such information. If passed, the bill would, among other things, require entities to disclose their data handling and sharing practices, and obtain express affirmative consent to use, collect, or disclose precise geolocation information.
3. S. 799 – The Commercial Privacy Bill of Rights Act of 2011, sponsored by Sen. John McCain (R-AZ) and Sen. John Kerry (D-MA), expressly includes “precise geographic location, at the same degree of specificity as a global positioning system or equivalent system” as “personally identifiable information” if combined with other express types of information about an individual including name, address, e-mail address, telephone number, etc.¹³ The bill is aimed at providing consumers with greater control over the collection and use of their personal information accessible through online offline channels. If passed, the bill would create baseline fair information practice protections including consumer notice prior to collection, and opt-in or opt-out consent mechanisms depending on the type of personal information collected and its intended use.
4. H.R. ____ [discussion draft] - Mobile Device Privacy Act, sponsored by Rep. Ed Markey (D-MA), would require mobile telephone sellers, service providers, manufacturers (including operating system manufacturers), and website operators (as applicable) to make certain consumer disclosures.¹⁴ These disclosures include: (a) the presence of monitoring software installed, or to be installed, on the consumer’s device, (b) the types of information the monitoring software is callable of collecting and transmitting, (c) the identity of any person to whom any information collected will be transmitted and of any other person with whom the information will be shared, and (d) how the information will be used.

¹² H.R. 611, 112th Cong. (2011), *available at* <http://www.gpo.gov/fdsys/pkg/BILLS-112hr611ih/pdf/BILLS-112hr611ih.pdf>.

¹³ S. 799, 112th Cong. (2011), *available at* <http://www.gpo.gov/fdsys/pkg/BILLS-112s799is/pdf/BILLS-112s799is.pdf>.

¹⁴ H.R. ____, 112th Cong. (2012) (discussion draft), *available at* http://markey.house.gov/sites/markey.house.gov/files/documents/Mobile%20Device%20Privacy%20Act%20--%20Rep.%20Markey%201-30-12_0.pdf.

IV. REGULATORY ACTIVITIES

A. FTC PRIVACY REPORT AND STATEMENTS

1. The FTC has taken a lead role, from a regulatory perspective, in enforcement and in tailoring broader Web-based consumer protection concepts to the mobile app environment.
2. In December 2010, the FTC released a preliminary FTC Staff privacy report proposing a new privacy framework.¹⁵ While taking a comprehensive approach to privacy, FTC Staff provided specific comments on the mobile environment stating, “[a]ll companies involved in information collection and sharing on mobile devices — carriers, operating system vendors, applications, and advertisers — should provide meaningful choice mechanisms for consumers.”¹⁶ Since the release of the preliminary report, location-based apps have come to the forefront of this discussion.
3. In subsequent testimony before Congress, the FTC has reaffirmed its role in regulating the mobile environment stating “[a]lthough there are no special laws applicable to mobile marketing that the FTC enforces, the FTC’s core consumer protection law — Section 5 of the FTC Act — prohibits unfair or deceptive practices in the mobile arena. This law applies to marketing in all media, whether traditional print, telephone, television, desktop computer, or mobile device.”¹⁷
4. With regard to location information, the FTC specifically has stated that “although the app may need location information, the app developer should carefully consider how long the location information should be retained to provide the requested service.”¹⁸
5. To further solidify its role as a primary enforcer in the mobile app environment, the FTC further stated that FTC “staff has a number of active investigations into privacy issues associated with mobile devices, including children’s privacy.”¹⁹

B. FTC ENFORCEMENT ACTIVITY, RULEMAKING, AND GUIDANCE

1. In August 2011, the FTC announced a settlement in its first enforcement action against an app developer over alleged children’s privacy violations. The action reinforced earlier statements from the FTC and was intended to send a message to

¹⁵ FTC Staff, *Protecting Consumer Privacy in an Era of Rapid Change* (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

¹⁶ *Id.* at 59.

¹⁷ FTC, *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before the United States Senate Committee on the Judiciary, Subcommittee for Privacy, Technology and the Law* at 3 (May 10, 2011), available at <http://www.ftc.gov/os/testimony/110510mobileprivacysenate.pdf>.

¹⁸ *Id.* at 10.

¹⁹ *Id.* at 8.

the mobile app market that the FTC is closely monitoring the industry for practices that violate consumer protection laws and privacy restrictions.

2. To settle claims that it collected children’s personal information without parental consent in violation of the Children’s Online Privacy Protection Act (“COPPA”), W3 Innovations, LLC d/b/a Broken Thumbs Apps, developer of “Emily Apps” paid a \$50,000 civil penalty and deleted all personal data collected by the developer, and has agreed to settlement provisions that extend for 20 years.²⁰
3. In October 2011, the FTC announced a settlement against a peer-to-peer file-sharing app developer that made both desktop and mobile apps over allegations that settings in its software would cause users to expose sensitive personal files stored on their computers and devices without reasonable notice to the user.
4. To settle the claims that it misled consumers into disclosing personal information stored on their computers and devices and that the app design unfairly harmed consumers, Frostwire LLC agreed to (a) not use default settings that share users’ files, (b) provide free app upgrades to correct unintended sharing, and (c) clearly disclose sharing options to users.²¹
5. FTC has proposed revisions to COPPA that would directly impact the mobile app market. In its proposed rule, the definition of “personal information” under COPPA would include geolocation information emitted by a child’s mobile or electronic device. This would expand the current location-based criteria that include “a home or other physical address including street name and name of a city or town.” This proposed change responds, in part, to concerns expressed by FTC and Congress over the extent to which mobile operators can collect user device location information.²²
6. FTC Staff has requested comments to the current Dot Com Disclosures Guide,²³ expressly acknowledging the growth of mobile marketing and the emergence of an “app” economy. Updated guidance will (a) facilitate the clear communication of material terms associated with mobile products and services; and (2) provide all participants in the mobile ecosystem with best practices on appropriate disclosures when conducting online advertising or engaging consumers through online channels such as social media.²⁴

²⁰ *United States v. W3 Innovations, LLC*, No. CV11-03958-PSG (N.D. Cal. Sept 08, 2011) (consent decree), available at <http://www.ftc.gov/os/caselist/1023251/110908w3order.pdf>.

²¹ *Federal Trade Commission v. Frostwire LLC*, No. 11-23643-CV-GRAHAM (S.D. Fla. Oct. 12, 2011 (stipulated final order), available at <http://www.ftc.gov/os/caselist/1123041/111012frostwirestip.pdf>.

²² Children’s Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (Sept. 27, 2011) (proposed rule; request for comment).

²³ FTC, *Dot Com Disclosures*, <http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf>.

²⁴ Press Release, *FTC Seeks Input for Revising Its Guidance to Businesses About Disclosures in Online Advertising* (May 26, 2011), available at <http://www.ftc.gov/opa/2011/05/dotcom.shtm>.

7. FTC released consumer guidance materials Understanding Mobile Apps that addresses mobile app basics, privacy, advertising, security, and user reviews on mobile platforms.²⁵

C. REGULATORY INQUIRIES AND HEARINGS

1. In April 2011, Pandora Media Inc.'s IPO filings with the SEC disclose a subpoena from a federal grand jury investigating whether smartphone apps share information about their users with advertisers and other third parties.²⁶
2. On April 25, 2011, the Illinois Attorney General sent a letter to Apple and Google seeking a meeting with both companies to discuss their device location-tracking practices.²⁷
3. On April 27, 2011, the Connecticut Attorney General sent a letter to Apple and Google asking whether the companies tracked consumer locations without permission.²⁸

V. KEY LAWSUITS: THE EMERGING LEGAL LANDSCAPE

A. UNIQUE DEVICE IDENTIFIERS AND LOCATION INFORMATION

1. *In re iPhone Application Litig.*²⁹ consolidates numerous actions brought against apple alleging violation of federal electronic communications laws, state unfair competition and deception laws, and common law claims.³⁰ The action was based on Apple's collection of unique device identifier information as well as location information, allegedly without the user's knowledge of such collection.
2. On September 20, 2011, the court dismissed the case finding that plaintiffs lacked standing because their complaint did not adequately alleged that they suffered any concrete injury. The case was dismissed without prejudice, so the plaintiffs may re-file if they can produce facts showing actual injury sufficient for standing.

²⁵ <http://www.ftc.gov/bcp/edu/microsites/onguard/articles/understandingmobileapps.shtml>.

²⁶ *Pandora Discloses Privacy-Related U.S. Inquiry Into Phone Apps*, N.Y. Times (Apr. 4, 2011), available at <http://www.nytimes.com/2011/04/05/technology/05pandora.html>.

²⁷ Press Release, *Attorney General Madigan Calls on Apple, Google to Address Mobile Device Privacy Concerns*, (Apr. 25, 2011), available at http://illinoisattorneygeneral.gov/pressroom/2011_04/20110425.html.

²⁸ Press Release, *Apple, Google Asked to Provide Information About Smartphone Tracking*, (Apr. 27, 2011), available at http://www.ct.gov/ag/lib/ag/press_releases/2011/042711applegoogle.pdf.

²⁹ *In re Apple iPhone Application Litig.*, No. 5:10-cv-05878-LHK (N.D. Cal. Filed Apr. 21, 2011) (first amended complaint).

³⁰ *See Lalo v. Apple, Inc.*, No. 10-cv-05878 (N.D. Cal. Filed Dec. 23, 2010); *Freeman v. Apple, Inc.*, 10-cv-05881 (N.D. Cal. Filed Dec. 23, 2010); *Chiu v. Apple, Inc.*, No. 5-cv-00407 (N.D. Cal. Filed Jan 27, 2011); *Rodimer v. Apple, Inc.*, No. 5-cv-00700 (N.D. Cal. Filed Feb. 15, 2011).

3. In *O’Flaherty v. Apple, Inc.*,³¹ plaintiff alleges Apple’s iOS 4 on mobile devices stores geolocation information and timestamp in unencrypted format on phone and on computers after device sync. The complaint does not focus on unique device identifiers (as found in *In re iPhone Application Litig.*) but addresses similar data collection and geolocation tracking without consent.
4. In *Brown v. Google, Inc.*,³² plaintiff alleges Google’s Android operating system on mobile devices stores geolocation information, timestamp and unique device identifier without consumer disclosure or consent.

VI. BEST PRACTICES

A. PRACTICAL GUIDANCE

1. The following best practices are based on legislative proposals and takeaways from Congressional hearings, regulatory enforcement actions and policy statements, guidance based on consumer concerns raised in private litigation, and industry sector recommendations.
2. App Design
 - a. Be mindful of the collection, purpose and retention of personal information, especially when it is linked to location-based information.
 - b. Take stock of the third parties that may have access to location-based information, especially if it is publicly available, such as metadata associated with a picture or tag applied by a user through the app.
 - c. Ensure that the app only collects as much data as you need for the app to work.
3. Consumer Experience
 - a. Evaluate the default settings for the app and whether they are consumer-friendly.
 - b. Ensure that there is an appropriate notice and consent mechanism in place for data usage and sharing.
4. Communication with Business Partners and Consumers
 - a. Discuss expectations and restrictions on how the app will function and any elements required by an application store (e.g., terms of use).
 - b. Provide easily-accessible disclosures in plain language to consumers.

³¹ No. 3:11-cv-00359-MJR-DGW (S.D. Ill. Filed Apr. 29, 2011), *transferred* No. 5:12-cv-00162 (N.D. Cal. Jan 18, 2012).

³² No. 2:11-cv-11867-AC-MAR (E.D. Mich. Filed Apr. 27, 2011).

- c. Consider whether such disclosures should be provided (i) at the time of download, (ii) within an application store on online presence, or (iii) when making a subsequent change to the application settings.
 - d. Note that the level of consumer interaction will differ based on the use of (i) privacy statements, (ii) terms of use, or (iii) just-in-time disclosures.
5. Contractual Protection
- a. Allocate risk appropriately among all the parties.
 - b. Businesses should ensure that app development contracts address key terms such as (i) the scope of data collected and permissible uses, (ii) approval of consumer disclosure language, (iii) representations regarding compliance with laws, project specifications, and policies/procedures, (iv) indemnification, and (v) limitation of liability provisions that reinforce obligations.

B. INDUSTRY AND PUBLIC INTEREST/PRIVACY GROUP MATERIALS

- 1. Industry and public interest/privacy group guidelines and best practices represent a growing body of resource materials.
 - a. CTIA Best Practices and Guidelines for Location-Based Services³³
 - b. Mobile Marketing Association (“MMA”) Global Code of Conduct,³⁴ Mobile Advertising Guidelines,³⁵ and Mobile Application Privacy Policy Framework³⁶
 - c. Center for Democracy & Technology (“CDT”) and Future of Privacy Forum (“FPF”) Best Practices for Mobile Applications Developers³⁷
 - d. TRUSTe Location-Aware Mobile Applications: Privacy Concerns & Best Practices³⁸
- 2. Although these guidelines may not have the force of law, many contracts in the mobile space require companies to comply with the guidelines.

³³ http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.

³⁴ <http://mmaglobal.com/codeofconduct.pdf>.

³⁵ <http://mmaglobal.com/mobileadvertising.pdf>.

³⁶ <http://mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps>

³⁷ <http://www.futureofprivacy.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf>

³⁸ http://www.truste.com/pdf/Location_Aware_Mobile_Applications.pdf



PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: <http://www.fcc.gov>
TTY: 1-888-835-5322

DA 11-857
Released: May 17, 2011

FCC STAFF TO HOST FORUM AIMED AT HELPING CONSUMERS NAVIGATE LOCATION-BASED SERVICES

WT Docket No. 11-84

Forum Date: June 28, 2011
Comments Due: July 8, 2011

The Federal Communications Commission's (FCC's) Wireless Telecommunications Bureau (the Bureau) in consultation with Federal Trade Commission (FTC) staff will hold a public education forum featuring representatives of telecommunications carriers, technology companies, consumer advocacy groups and academia on June 28, 2011, exploring how consumers can be both smart and secure when realizing the benefits of Location Based Services (LBS).

Topics will include: how LBS works; benefits and risks of LBS; consumer DOs and DON'Ts; industry best practices; and what parents should know about location tracking when their children use mobile devices.

The event will be held from 9:00 a.m. to 3:00 p.m., at FCC Headquarters, 445 12th Street, SW, Washington DC, 20554. This session, as well as comments received in response to this Public Notice, will inform a forthcoming staff report on LBS.

Over the last few years, LBS have become an important part of the mobile market and a boon to the economy. Commercial location-based services include applications that help consumers find the lowest-priced product nearby or the nearest restaurant. Additionally, innovations in the use of location technology have the potential to open up new services for consumers and to aid public safety entities with emergency response. But recent reports have raised concerns about the location-based information that is gathered when consumers use mobile devices. While the use of location data has spurred innovation, the FCC's National Broadband Plan recognizes that consumer apprehension about privacy can also act as a barrier to the adoption and utilization of broadband and mobile devices.¹ Clear information and public education can help consumers better understand these services. Indeed, both the staff at the FTC and the Department of Commerce recently issued separate reports noting the growing importance of addressing concerns about location privacy.²

¹ Federal Communications Commission, *Connecting America: The National Broadband Plan*, FCC Staff Report, at 54 (Mar. 2010), <http://download.broadband.gov/plan/national-broadband-plan.pdf>.

² See FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers*, Preliminary Staff Report, at 47 (Dec. 2010), <http://www.ftc.gov/opa/2010/12/privacyreport.shtml>; Internet Policy Task Force, Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Green Paper, at 63 (Dec. 2010), http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

To address these and other privacy issues, FCC Chairman Julius Genachowski and FTC Chairman Jon Leibowitz last summer established a Joint Privacy Task Force through which the two agencies are able to discuss and address consumer concerns and encourage smart innovation in this space.³ Over the last several months, the FCC has also had an internal working group examining the privacy implications of the increased use of LBS and related services.

We encourage interested parties to help inform the discussion and a subsequent staff-level report by filing comments. Additional details regarding the session, including the agenda and information about the panelists, will be provided in a future release.

FILING PROCEDURES

Interested parties may file comments using the Commission's Electronic Comment Filing System (ECFS) or by filing paper copies.⁴ Comments filed through the ECFS can be sent as an electronic file via the Internet to <http://www.fcc.gov/cgb/ecfs/>. Generally, only one copy of an electronic submission must be filed. If multiple docket or rulemaking numbers appear in the caption of the proceeding, commenters must transmit one electronic copy of the comments to each docket or rulemaking number referenced in the caption. In completing the transmittal screen, commenters should include their full name, U.S. Postal Service mailing address, and the applicable docket or rulemaking numbers. All filings concerning this Public Notice should refer to WT Docket No 11-84. Parties may also submit an electronic comment by Internet e-mail. To get filing instructions for e-mail comments, commenters should send an e-mail to ecfs@fcc.gov, and should include the following words in the body of the message, "get form." A sample form and directions will be sent in reply. Parties who choose to file by paper must file an original and four copies of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, commenters must submit two additional copies for each additional docket or rulemaking number.

Paper filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail (although we continue to experience delays in receiving U.S. Postal Service mail). All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission. **Parties are strongly encouraged to file comments electronically using the Commission's ECFS.**

- Effective December 28, 2009, all hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours at this location are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building. **PLEASE NOTE:** The Commission's former filing location at 236 Massachusetts Avenue, NE is permanently closed.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.
- U.S. Postal Service first-class, Express, and Priority mail should be addressed to 445 12th Street, SW, Washington DC 20554.

³ See *Consumer Online Privacy: Hearing Before S. Comm. on Commerce, Science, and Transportation*, 111th Cong. at 2 (July 27, 2010) (statement of Julius Genachowski, Chairman, Federal Communications Commission), available at <http://fcc.us/kmN0J6>.

⁴ See *Electronic Filing of Documents in Rulemaking Proceedings*, GC Docket No. 97-113, Report and Order, 13 FCC Rcd 11322 (1998).

Parties shall also serve one copy with the Commission's copy contractor, Best Copy and Printing, Inc. (BCPI), Portals II, 445 12th Street, S.W., Room CY-B402, Washington, D.C. 20554, (202) 488-5300, or via e-mail to fcc@bcpiweb.com.

Documents in WT Docket No. 11-84 will be available for public inspection and copying during business hours at the FCC Reference Information Center, Portals II, 445 12th St. S.W., Room CY-A257, Washington, DC 20554. The documents may also be purchased from BCPI, telephone (202) 488-5300, facsimile (202) 488-5563, TTY (202) 488-5562, e-mail fcc@bcpiweb.com.

To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

For purposes of the Commission's *ex parte* rules, the forum and comments submitted in WT Docket No. 11-84, will be treated as exempt.⁵ *Ex parte* presentations may be freely made and need not be disclosed on the record, although filing in the record is encouraged.⁶ We find that this approach is justified because, as in a notice of inquiry proceeding, the public interest will best be served by encouraging free communication between the Commission and the public and because the nature of this project obviates any risk that interested persons will be prejudiced unless they receive notice of *ex parte* presentations. To the extent that presentations related to this project address the merits of other permit-but-disclose proceedings, appropriate disclosures should be made in each other covered proceeding. In the event that this project develops to the point where a notice of proposed rulemaking is issued, we anticipate that the status of any such proceeding will be changed to permit-but-disclose, as is the norm when a notice of proposed rulemaking is issued.

Audio/video coverage of the meeting will be broadcast live with open captioning over the Internet from the FCC's web page at www.fcc.gov/live. The FCC's webcast is free to the public. Those who watch the live video stream of the event may email event-related questions to livequestions@fcc.gov. Depending on the volume of questions and time constraints, the panel moderators will work to respond to as many questions as possible during the workshop.

Reasonable accommodations for persons with disabilities are available upon request. Please include a description of the accommodation you will need. Individuals making such requests must include their contact information should FCC staff need to contact them for more information. Requests should be made as early as possible. Please send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau: 202-418-0530 (voice), 202-418-0432 (TTY).

For additional information, please contact Christina Clearwater or Nicole McGinnis of the Spectrum and Competition Policy Division, Wireless Telecommunications Bureau. Christina Clearwater can be reached at 202-418-1893 or by email at Christina.Clearwater@fcc.gov; Nicole McGinnis can be reached at 202-418-2877 or by email at Nicole.McGinnis@fcc.gov.

-FCC-

⁵ See 47 C.F.R. § 1.1200(a) (giving the Commission and its staff discretion to determine the *ex parte* procedures in a particular proceeding).

⁶ See 47 C.F.R. § 1.1204(b).

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 11-23643-CV-GRAHAM

**CLOSED
CIVIL
CASE**

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

FROSTWIRE LLC, *et al.*,

Defendants.

STIPULATED FINAL ORDER FOR PERMANENT INJUNCTION

Plaintiff, the Federal Trade Commission (“Plaintiff” or “Commission”), filed a Complaint for Permanent Injunction and Other Equitable Relief (“Complaint”) against the Defendants, pursuant to Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 53(b). The Commission and Defendants stipulate to the entry of this Final Order for Permanent Injunction (“Order”) to resolve all matters in dispute in this action between them. Accordingly, it is hereby ordered as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter and over all of the parties. Venue is proper as to all parties in this District.
2. The Complaint states claims upon which relief may be granted against Defendants under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).
3. The activities of Defendants are in or affecting commerce, as defined in Section 4 of the

FTC Act, 15 U.S.C. § 44.

4. Defendants waive all rights to appeal or otherwise challenge or contest the validity of this Order. Defendants also waive any claims they may have held under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action to the date of the Order.
5. Each party shall bear its own costs and attorneys' fees.
6. Defendants do not admit any allegations in the Complaint, except for facts necessary to establish jurisdiction, and as otherwise specifically stated in this Order.

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

“Actions substantially equivalent to” means clicks, touches, or similar actions that are the same as, or highly similar to, and presented in the same location as, those the consumer previously took to change the software program setting; that are equal to or less in number than those previous actions; and that are explained and described to the consumer in a format and using terminology consistent with those used to explain how to make the previous change.

“Affirmatively select” means to choose by checking a box or touching a button or icon on a computer screen that is not pre-selected as the default option, or by taking a substantially similar action.

“Clear(ly) and prominent(ly)” means:

- a. In textual communications (*e.g.*, words displayed on a computer screen), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

- b. In communications disseminated orally or through audible means (*e.g.*, streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
- c. In communications disseminated through video means (*e.g.*, streaming video), the required disclosures are in writing in a form consistent with subparagraph (a) of this definition and appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication;
- d. In communications made through interactive media (*e.g.*, online services and software), the required disclosures are unavoidable and presented in a form consistent with subparagraph (a) of this definition, in addition to any audio or video presentation of them; and
- e. In all instances, the required disclosures are: (1) presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures used in any communication with the consumer.

“Computer” means any desktop or laptop computer, handheld device, telephone, smartphone, tablet, or other electronic device that has a platform on which to download, install, or run any software program, code, script, or other content.

“Corporate Defendant” means Frostwire LLC and its successors and assigns.

“Defendants” means the Corporate Defendant and Individual Defendant, individually, collectively, or in any combination.

“File-sharing application” means any software program that, when installed and running on a computer, can enable the users of other computers running the same program or a compatible program (known as “peer” computers) to search for and copy files from that computer, and includes FrostWire Desktop and FrostWire for Android.

“File-sharing network” means a computer network formed when multiple, individual peer computers running file-sharing applications communicate with each other and enable peer computers to search for and copy files from each other, including the “Gnutella” file-sharing network and any networks formed when multiple computers communicate through one or more common wireless access devices.

“FrostWire Desktop” means any version of the software program Defendants have marketed and/or distributed to the public under the name “FrostWire,” including through www.frostwire.com and www.download.com, that can be installed on computers running various versions of the Microsoft Windows operating system and other operating systems, but not including FrostWire for Android.

“FrostWire for Android” means any version of the software program Defendants have marketed and/or distributed to the public under the name “FrostWire for Android,” including through www.frostwire.com, the Android Marketplace, and www.amazon.com, that can be installed on computers running various versions of the Android mobile operating system.

“Including” means including without limitation.

“Individual Defendant” means Angel Leon.

“Legacy Version” means any version of Frostwire Desktop distributed in commerce by Defendants prior to June 10, 2011, or any version of Frostwire for Android distributed in commerce by Defendants prior to May 6, 2011.

“**Person(s)**” means a natural person, an organization, or other legal entity, including a corporation, partnership, sole proprietorship, limited liability company, association, cooperative, or any other group or combination acting as an entity.

To “**share**” files means to make files available for searching, browsing, and/or copying by third parties, including through any file-sharing network.

“**User-originated files**” means any files stored on a computer prior to installation of a file-sharing application and any files subsequently stored on that computer that a user has not downloaded by means of that file-sharing application, including any files created, downloaded, or saved through the use of any other software program on the computer, and including any files copied to a computer running FrostWire for Android from a computer running FrostWire Desktop using those two programs.

ORDER

I.

PROHIBITION ON MISREPRESENTATIONS

IT IS HEREBY ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all other persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, in connection with the advertising, distribution, downloading, installation, or operation of any file-sharing application in commerce, are hereby permanently restrained and enjoined from misrepresenting, or assisting others in misrepresenting, expressly or by implication:

- A. that consumers’ computers will not publicly share, or are not publicly sharing, files consumers download or have downloaded from the Gnutella network, including through

the FrostWire Desktop “Save Folder and Shared Folders” dialog box and “Options-Sharing” box;

- B. what files the file-sharing application will share or the audience with whom they will be shared;
- C. how consumers can initiate or stop sharing files when they install or run the file-sharing application on a computer; or
- D. any other material fact about how the file-sharing application operates.

II.

REQUIRED DISCLOSURES AND DEFAULTS RELATING TO THE SHARING OF DOWNLOADED FILES

IT IS FURTHER ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all other persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, distributing, enabling the downloading or installation of, or causing to operate any file-sharing application in commerce unless:

- A. before the consumer installs or runs the application, the application:
 - 1. clearly and prominently discloses to the consumer which files downloaded from a file-sharing network, if any, it will share and the audience with whom those files will be shared;
 - 2. requires the consumer first to affirmatively select which files downloaded from the network, if any, to share;

3. clearly and prominently discloses how the consumer can stop sharing files the consumer downloads from the network; and
- B. after the application is installed and running, the application:
1. allows the consumer to disable sharing of files previously and subsequently downloaded from the network immediately upon taking actions substantially equivalent to those required to affirmatively select such files for sharing after the application is installed; and
 2. provides a clearly labeled link or distinctive icon linking from the application's listings of shared files to clear and prominent written, graphical, and audiovisual instructions about how to disable sharing of files.

III.

REQUIREMENTS RELATING TO USER-ORIGINATED FILES AND DEFAULT SETTINGS

IT IS FURTHER ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all other persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, distributing, enabling the downloading or installation of, or causing to operate any file-sharing application in commerce that can share user-originated files, unless any such sharing can be enabled only after the application is completely installed and set up, and the application:

- A. clearly and prominently discloses to the consumer which user-originated files, if any, the consumer can choose to share using the application, and the audience with whom those files would be shared;

- B. is set, by default, to require the consumer to affirmatively select the specific, individual files to be shared, and to confirm after clear and prominent disclosure that selected files will be shared;
- C. enables consumers to change the default settings described in Subsection III.B, above, provided that the application does not prompt the consumer to change those default settings, and only if the consumer:
 - 1. affirmatively selects an option to do so after clear and prominent disclosure about the effect of the change and confirms the change through an affirmative selection;
 - 2. must affirmatively select any groups of files to be shared;
 - 3. after making any change to a default setting described in Subsection III.B, above, can re-enable the default setting immediately upon taking actions substantially equivalent to those required to change it;
- D. allows the consumer to disable sharing of any files or groups of files immediately upon taking actions substantially equivalent to those required to select them for sharing; and
- E. provides a clearly labeled link or distinctive icon linking from the application's listings of shared files to clear and prominent written, graphical, and audiovisual instructions about how to disable sharing of files.

IV.

REQUIREMENTS REGARDING LEGACY VERSIONS

IT IS FURTHER ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all other persons or entities in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, are permanently restrained and enjoined from promoting, selling, or

distributing, or assisting others in so doing, any Legacy Version of Frostwire Desktop or Frostwire for Android. **It is further ordered** that, within ten (10) business days of the entry of this order, Defendants shall, to the extent that they have not done so previously, transmit or cause to be transmitted:

- A. to all computers running any Legacy Version of FrostWire Desktop:
 - 1. code that, when installed, designates all “Individually shared” files on those computers not to be shared by the application unless consumers using those computers affirmatively select them to be shared, and upgrades the application to comply with the requirements of Sections I-III of this Order; and
 - 2. a clear and prominent notice to consumers using those computers that advises them to install the code described in Subsection IV.A.1 of this Order, and that includes a clearly labeled command button or link enabling consumers to initiate that installation; and

- B. to all computers running any Legacy Version of FrostWire for Android:
 - 1. code that, when installed, designates all previously shared files on those computers not to be shared by the application unless consumers using those computers affirmatively select them to be shared, and upgrades the application to comply with the requirements of Sections I-III of this Order; and
 - 2. a clear and prominent notice to consumers using those computers that advises them to install the code described in Subsection IV.B.1 of this Order, and that includes a clearly labeled command button or link enabling consumers to initiate that installation.

V.

COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring and investigating compliance with any provision of this Order:

- A. Within ten (10) days of receipt of written notice from a representative of the Commission, Defendants each shall submit additional written reports, which are true and accurate and sworn to under penalty of perjury; produce documents for inspection and copying; appear for deposition; and provide entry during normal business hours to any business location in each Defendant's possession or direct or indirect control to inspect the business operation;
- B. In addition, the Commission is authorized to use all other lawful means, including but not limited to:
 - 1. obtaining discovery from any person, without further leave of court, using the procedures prescribed by Fed. R. Civ. P. 30, 31, 33, 34, 36, 45 and 69;
 - 2. having its representatives pose as consumers and suppliers to Defendants, their employees, or any other entity managed or controlled in whole or in part by any Defendant, without the necessity of identification or prior notice; and
- C. Defendants each shall permit representatives of the Commission to interview any employer, consultant, independent contractor, representative, agent, or employee who has agreed to such an interview, relating in any way to any conduct subject to this Order.

The person interviewed may have counsel present.

Provided however, that nothing in this Order shall limit the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1, to

obtain any documentary material, tangible things, testimony, or information relevant to unfair or deceptive acts or practices in or affecting commerce (within the meaning of 15 U.S.C. § 45(a)(1)).

VI.

COMPLIANCE REPORTING

IT IS FURTHER ORDERED that, in order that compliance with the provisions of this Order may be monitored:

- A. For a period of three (3) years from the date of entry of this Order,
 1. Individual Defendant shall notify the Commission of the following:
 - a. Any changes in his residence, mailing addresses, and telephone numbers, within ten (10) days of the date of such change;
 - b. Any changes in his employment status (including self-employment), and any change in his ownership in any business entity, within ten (10) days of the date of such change. Such notice shall include the name and address of each business that he is affiliated with, employed by, creates or forms, or performs services for; a detailed description of the nature of the business; and a detailed description of his duties and responsibilities in connection with the business or employment; and
 - c. Any changes in his name or use of any aliases or fictitious names within ten (10) days of the date of such change;
 2. Defendants shall notify the Commission of any changes in structure of the Corporate Defendant or any business entity that any Defendant directly or indirectly controls, or has an ownership interest in, that may affect compliance

obligations arising under this Order, including but not limited to: incorporation or other organization; a dissolution, assignment, sale, merger, or other action; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; or a change in the business name or address, at least thirty (30) days prior to such change, *provided* that, with respect to any such change in the business entity about which a Defendant learns less than thirty (30) days prior to the date such action is to take place, such Defendant shall notify the Commission as soon as is practicable after obtaining such knowledge.

B. Sixty (60) days after the date of entry of this Order, Defendants each shall provide a written report to the FTC, which is true and accurate and sworn to under penalty of perjury, setting forth in detail the manner and form in which they have complied and are complying with this Order. This report shall include, but not be limited to:

1. For Individual Defendant:
 - a. his then-current residence address, mailing addresses, and telephone numbers;
 - b. his then-current employment status (including self-employment), including the name, addresses, and telephone numbers of each business that he is affiliated with, employed by, or performs services for; a detailed description of the nature of the business; and a detailed description of his duties and responsibilities in connection with the business or employment; and
 - c. Any other changes required to be reported under Subsection A of this Section.

2. For all Defendants:
 - a. A copy of each acknowledgment of receipt of this Order, obtained pursuant to the Section titled "Distribution of Order";
 - b. Any other changes required to be reported under Subsection A of this Section.
- C. Each Defendant shall notify the Commission of the filing of a bankruptcy petition by such Defendant within fifteen (15) days of filing.
- D. For the purposes of this Order, Defendants shall, unless otherwise directed by the Commission's authorized representatives, send by overnight courier (not the U.S. Postal Service) all reports and notifications to the Commission that are required by this Order to:

Associate Director for Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
RE: FTC v. Frostwire LLC

Provided that, in lieu of overnight courier, Defendants may send such reports or notifications by first-class mail, but only if Defendants contemporaneously send an electronic version of such report or notification to the Commission at DEbrief@ftc.gov.

- E. For purposes of the compliance reporting and monitoring required by this Order, the Commission is authorized to communicate directly with each Defendant.

VII.

RECORDKEEPING

IT IS FURTHER ORDERED that, for a period of six (6) years from the date of entry of

this Order, each Defendant, in connection with any business where (1) such Defendant is the majority owner, or directly or indirectly manages or controls the business, and (2) the business is engaged in or assists others engaged in the development, marketing, sale, or distribution in commerce of any file-sharing application, and their agents, employees, officers, corporations, successors and assigns, are hereby restrained and enjoined from failing to create and/or retain the following records:

- A. Accounting records that reflect revenues generated relating to the downloading, installation, or use of file-sharing applications, and the disbursement of such revenues; and, to the extent such information is obtained in the ordinary course of business, records that reflect the number of downloads and installations of file-sharing applications;
- B. Personnel records accurately reflecting: the name, address, and telephone number of each person who is employed in any capacity by such business, including as an independent contractor, and who participates in the conduct specified in Sections I-IV; that person's job title or position; the date upon which the person commenced work; and the date and reason for the person's termination, if applicable;
- C. Complaints and refund requests (whether received directly or indirectly, such as through a third party) and any responses to those complaints or requests;
- D. All records and documents necessary to demonstrate full compliance with each provision of this Order, including but not limited to:
 1. copies of acknowledgments of receipt of this Order required by the Sections titled "Distribution of Order" and "Acknowledgment of Receipt of Order";
 2. all reports submitted to the FTC pursuant to the Section titled "Compliance Reporting"; and

3. all records and documents that contradict, qualify, or call into question Defendants' compliance with this Order; and

E. An executable copy of each materially different version of each file-sharing application that any Defendant, whether acting directly or indirectly, distributes or makes available for download, and any programmer documentation, developer guides, specification documents, version histories and change logs, application store documentation or submissions, application store descriptions and disclosures, terms of service, end user license agreements, frequently asked questions, instructional materials, privacy policies, domain name registrations, and online service agreements associated with those versions.

VIII.

DISTRIBUTION OF ORDER

IT IS FURTHER ORDERED that, for a period of three (3) years from the date of entry of this Order, Defendants shall deliver copies of the Order as directed below:

A. Corporate Defendant: The Corporate Defendant must deliver a copy of this Order to (1) all of its principals, officers, directors, and managers; (2) all of its employees, agents, and representatives who engage in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting." For current personnel, delivery shall be within five (5) days of service of this Order upon such Defendant. For new personnel, delivery shall occur prior to their assuming their responsibilities. For any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting," delivery shall be at least ten (10) days prior to the change in structure.

- B. Individual Defendant as control person: For any business that Individual Defendant controls, directly or indirectly, or in which he has a majority ownership interest, he must deliver a copy of this Order to (1) all principals, officers, directors, and managers of that business; (2) all employees, agents, and representatives of that business who engage in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting." For current personnel, delivery shall be within five (5) days of service of this Order upon Individual Defendant. For new personnel, delivery shall occur prior to their assuming their responsibilities. For any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting," delivery shall be at least ten (10) days prior to the change in structure.
- C. Defendants must secure a signed and dated statement acknowledging receipt of the Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this Section.

IX.

ACKNOWLEDGMENT OF RECEIPT OF ORDER

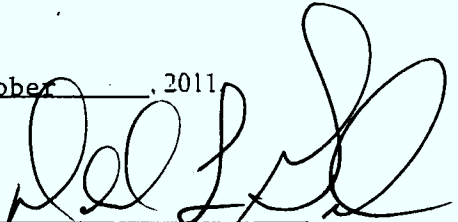
IT IS FURTHER ORDERED that each Defendant, within five (5) business days of receipt of this Order as entered by the Court, must submit to the Commission a truthful sworn statement acknowledging receipt of this Order.

X.

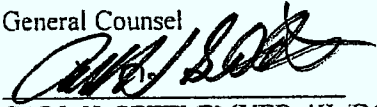
RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order. The Clerk shall **CLOSE** this case for administrative purposes only.

IT IS SO ORDERED, this 12th day of October, 2011

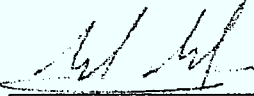

DONALD L. GRAHAM
UNITED STATES DISTRICT JUDGE


SO STIPULATED:

WILLARD K. TOM
General Counsel

CARL H. SETTLEMYER, III (DC Bar #454272)
KIAL S. YOUNG (Mass. BBO #633515)
Federal Trade Commission
600 Pennsylvania Avenue, N.W., NJ-3212
Washington, DC 20580
(202) 326-2019 (direct)
(202) 326-3259 (facsimile)
csettlemyer@ftc.gov / kyoun@ftc.gov


Dated: October 7, 2011

ATTORNEYS FOR PLAINTIFF

FROSTWIRE LLC
By: 
Its: Melinger
Dated: 7/1/2011

ANGEL LEON

Dated: 7/1/2011

APPROVED AS TO CONTENT AND FORM:


EDWARD F. GLYNN, JR.
CHRISTOPHER S. CROOK
Venable LLP
575 7th Street, N.W.
Washington, DC 20004
(202) 344-4805 (direct)
(202) 344-8300 (facsimile)
EFGlynn@venable.com /
CSCrook@venable.com

Dated: 7/1/2011

ATTORNEYS FOR DEFENDANTS



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Privacy and Identity Protection

**CERTIFIED MAIL
RETURN RECEIPT REQUESTED**

January 25, 2012

Everify, Inc.
d/b/a Police Records
Attn. Alon Cohen
745 Boylston Street, Suite 202
Boston, MA 02116

Dear Mr. Cohen:

This letter concerns your company's mobile application(s) that may be in violation of the Fair Credit Reporting Act ("FCRA"),¹ a federal law enforced by the Federal Trade Commission ("FTC").

Under the FCRA, a company is a consumer reporting agency ("CRA") if it assembles or evaluates information on consumers for the purpose of furnishing "consumer reports" to third parties.² Consumer reports include information that relates to an individual's character, reputation or personal characteristics and are used or expected to be used for employment, housing, credit, or other similar purposes. For example, when companies provide information to employers regarding current or prospective employees' criminal histories, they are providing "consumer reports" because the data involves the individuals' character, general reputation, or personal characteristics. Such companies, therefore, are acting as CRAs in this capacity and must comply with the FCRA.

CRAs must comply with several different FCRA provisions, including taking reasonable steps to ensure the maximum possible accuracy of the information provided in consumer reports.³ A CRA must also provide those who use its consumer reports with information about their obligations under the FCRA.⁴ In the case of reports provided for employment purposes, for example, the CRA must provide employers with information regarding their obligation to provide employees or applicants with notice of any adverse action taken on the basis of these reports, and to notify them of their rights to copies of the reports and to a free reinvestigation of

¹ 15 U.S.C. § 1681 *et seq.*

² 15 U.S.C. § 1681a(f).

³ 15 U.S.C. § 1681e(b).

⁴ 15 U.S.C. § 1681e(d).

information the consumer believes to be in error. A model notice is available in 16 Code of Federal Regulations § 698, Appendix H, which can be found at <http://www.ftc.gov/os/2004/11/041119factaapph.pdf>.

At least one of your company's mobile applications involves background screening reports that include criminal histories. Employers are likely to use such criminal histories when screening job applicants. If you have reason to believe that your reports are being used for employment or other FCRA purposes,⁵ you and your customers who are using the reports for such purposes must comply with the FCRA. This is true even if you have a disclaimer on your website indicating that your reports should not be used for employment or other FCRA purposes. We would evaluate many factors to determine if you had a reason to believe that a product is used for employment or other FCRA purposes, such as advertising placement and customer lists. At this time, we have not made a determination as to whether your company is violating the FCRA. However, we encourage you to review your mobile applications and your policies and procedures for compliance with the FCRA. You may find the full text of the FCRA and more information about the FCRA at <http://www.ftc.gov/os/statutes/fcrajump.shtm>.

The Commission reserves the right to take action against you based on past or future law violations; your practices also may be subject to laws enforced by other federal, state, or local law enforcement agencies. A violation of the FCRA may result in legal action by the FTC, in which it is entitled to seek injunctive relief and/or monetary penalties of up to \$3,500 per violation.⁶

If you have any questions, please call Anthony Rodriguez at (202) 326-2757.

Sincerely,



Maneesha Mithal
Associate Director

⁵ The FCRA also governs the potential use of the reports for, among other things, tenant screening purposes, and determining eligibility for credit or insurance.

⁶ See, e.g., *U.S. v. Teletrack, Inc.*, Case No. 1:11-CV-2060 (N.D. Ga. June 27, 2011) (consent agreement for civil penalties for \$1.8 million for violations of the FCRA).



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Privacy and Identity Protection

**CERTIFIED MAIL
RETURN RECEIPT REQUESTED**

January 25, 2012

InfoPay, Inc.
d/b/a Criminal Pages
Attn. Daniel Dechamps
50 Corporate Avenue
Plainville, CT 06062

Dear Mr. Dechamps:

This letter concerns your company's mobile application(s) that may be in violation of the Fair Credit Reporting Act ("FCRA"),¹ a federal law enforced by the Federal Trade Commission ("FTC").

Under the FCRA, a company is a consumer reporting agency ("CRA") if it assembles or evaluates information on consumers for the purpose of furnishing "consumer reports" to third parties.² Consumer reports include information that relates to an individual's character, reputation or personal characteristics and are used or expected to be used for employment, housing, credit, or other similar purposes. For example, when companies provide information to employers regarding current or prospective employees' criminal histories, they are providing "consumer reports" because the data involves the individuals' character, general reputation, or personal characteristics. Such companies, therefore, are acting as CRAs in this capacity and must comply with the FCRA.

CRAs must comply with several different FCRA provisions, including taking reasonable steps to ensure the maximum possible accuracy of the information provided in consumer reports.³ A CRA must also provide those who use its consumer reports with information about their obligations under the FCRA.⁴ In the case of reports provided for employment purposes, for example, the CRA must provide employers with information regarding their obligation to provide employees or applicants with notice of any adverse action taken on the basis of these

¹ 15 U.S.C. § 1681 *et seq.*

² 15 U.S.C. § 1681a(f).

³ 15 U.S.C. § 1681e(b).

⁴ 15 U.S.C. § 1681e(d).

reports, and to notify them of their rights to copies of the reports and to a free reinvestigation of information the consumer believes to be in error. A model notice is available in 16 Code of Federal Regulations § 698, Appendix H, which can be found at <http://www.ftc.gov/os/2004/11/041119factaapph.pdf>.

At least one of your company's mobile applications involves background screening reports that include criminal histories. Employers are likely to use such criminal histories when screening job applicants. If you have reason to believe that your reports are being used for employment or other FCRA purposes,⁵ you and your customers who are using the reports for such purposes must comply with the FCRA. This is true even if you have a disclaimer on your website indicating that your reports should not be used for employment or other FCRA purposes. We would evaluate many factors to determine if you had a reason to believe that a product is used for employment or other FCRA purposes, such as advertising placement and customer lists. At this time, we have not made a determination as to whether your company is violating the FCRA. However, we encourage you to review your mobile applications and your policies and procedures for compliance with the FCRA. You may find the full text of the FCRA and more information about the FCRA at <http://www.ftc.gov/os/statutes/fcrajump.shtm>.

The Commission reserves the right to take action against you based on past or future law violations; your practices also may be subject to laws enforced by other federal, state, or local law enforcement agencies. A violation of the FCRA may result in legal action by the FTC, in which it is entitled to seek injunctive relief and/or monetary penalties of up to \$3,500 per violation.⁶

If you have any questions, please call Anthony Rodriguez at (202) 326-2757.

Sincerely,



Maneesha Mithal
Associate Director

⁵ The FCRA also governs the potential use of the reports for, among other things, tenant screening purposes, and determining eligibility for credit or insurance.

⁶ See, e.g., *U.S. v. Teletrack, Inc.*, Case No. 1:11-CV-2060 (N.D. Ga. June 27, 2011) (consent agreement for civil penalties for \$1.8 million for violations of the FCRA).

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Privacy and Identity Protection

**CERTIFIED MAIL
RETURN RECEIPT REQUESTED**

January 25, 2012

Intelligator, Inc.
Attn. Amine Mamoun
P.O. Box 821650
Vancouver, WA 98682

Dear Mr. Mamoun:

This letter concerns your company's mobile application(s) that may be in violation of the Fair Credit Reporting Act ("FCRA"),¹ a federal law enforced by the Federal Trade Commission ("FTC").

Under the FCRA, a company is a consumer reporting agency ("CRA") if it assembles or evaluates information on consumers for the purpose of furnishing "consumer reports" to third parties.² Consumer reports include information that relates to an individual's character, reputation or personal characteristics and are used or expected to be used for employment, housing, credit, or other similar purposes. For example, when companies provide information to employers regarding current or prospective employees' criminal histories, they are providing "consumer reports" because the data involves the individuals' character, general reputation, or personal characteristics. Such companies, therefore, are acting as CRAs in this capacity and must comply with the FCRA.

CRAs must comply with several different FCRA provisions, including taking reasonable steps to ensure the maximum possible accuracy of the information provided in consumer reports.³ A CRA must also provide those who use its consumer reports with information about their obligations under the FCRA.⁴ In the case of reports provided for employment purposes, for example, the CRA must provide employers with information regarding their obligation to provide employees or applicants with notice of any adverse action taken on the basis of these reports, and to notify them of their rights to copies of the reports and to a free reinvestigation of

¹ 15 U.S.C. § 1681 *et seq.*

² 15 U.S.C. § 1681a(f).

³ 15 U.S.C. § 1681e(b).

⁴ 15 U.S.C. § 1681e(d).

information the consumer believes to be in error. A model notice is available in 16 Code of Federal Regulations § 698, Appendix H, which can be found at <http://www.ftc.gov/os/2004/11/041119factaapph.pdf>.

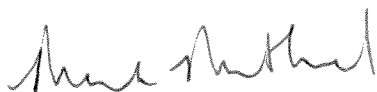
At least one of your company's mobile applications involves background screening reports that include criminal histories. Employers are likely to use such criminal histories when screening job applicants. If you have reason to believe that your reports are being used for employment or other FCRA purposes,⁵ you and your customers who are using the reports for such purposes must comply with the FCRA. This is true even if you have a disclaimer on your website indicating that your reports should not be used for employment or other FCRA purposes.

We would evaluate many factors to determine if you had a reason to believe that a product is used for employment or other FCRA purposes, such as advertising placement and customer lists. At this time, we have not made a determination as to whether your company is violating the FCRA. However, we encourage you to review your mobile applications and your policies and procedures for compliance with the FCRA. You may find the full text of the FCRA and more information about the FCRA at <http://www.ftc.gov/os/statutes/fcrajump.shtm>.

The Commission reserves the right to take action against you based on past or future law violations; your practices also may be subject to laws enforced by other federal, state, or local law enforcement agencies. A violation of the FCRA may result in legal action by the FTC, in which it is entitled to seek injunctive relief and/or monetary penalties of up to \$3,500 per violation.⁶

If you have any questions, please call Anthony Rodriguez at (202) 326-2757.

Sincerely,



Maneesha Mithal
Associate Director

⁵ The FCRA also governs the potential use of the reports for, among other things, tenant screening purposes, and determining eligibility for credit or insurance.

⁶ See, e.g., *U.S. v. Teletrack, Inc.*, Case No. 1:11-CV-2060 (N.D. Ga. June 27, 2011) (consent agreement for civil penalties for \$1.8 million for violations of the FCRA).

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

on

**PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS,
CELL PHONES AND YOUR PRIVACY**

Before the

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE FOR PRIVACY, TECHNOLOGY AND THE LAW

Washington, D.C.

May 10, 2011

Chairman Franken, Ranking Member Coburn, and members of the Subcommittee, my name is Jessica Rich and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate this opportunity to appear before you today to discuss the Commission’s efforts to protect consumers’ privacy in the mobile arena.

This testimony first broadly surveys the growth of the mobile marketplace and the Commission’s response to this developing industry. Second, it highlights four of the Commission’s recent law enforcement actions in the mobile arena, one involving statements that a public relations agency made in the iTunes mobile application store, another involving unsolicited commercial texts, and two recent privacy enforcement actions involving Google and Twitter, major companies in the mobile arena. Finally, it describes the Commission’s efforts to address the privacy challenges of these new, and often very personal technologies, including a discussion of how mobile technology is addressed in the privacy framework recently proposed by FTC staff.

I. The Mobile Marketplace

Mobile technology is exploding with a range of new products and services for consumers. According to the wireless telecommunications trade association, CTIA, the wireless penetration rate reached 96 percent in the United States by the end of last year.² Also by that

¹ While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

² See CTIA Wireless Quick Facts, *available at* www.ctia.org/advocacy/research/index.cfm/aid/10323.

same time, 27 percent of U.S. mobile subscribers owned a smartphone,³ which is a wireless phone with more powerful computing abilities and connectivity than a simple cell phone. Such mobile devices are essentially handheld computers that can not only make telephone calls, but also offer web browsing, e-mail, and a broad range of data services. These new popular mobile devices allow consumers to handle a multitude of tasks in the palm of their hands and offer Internet access virtually anywhere.

Companies are increasingly using this new mobile medium to provide enhanced benefits to consumers, whether to provide online services or content or to market other goods or services.⁴ Consumers can search mobile web sites to get detailed information about products, or compare prices on products they are about to purchase while standing in the check-out line. Consumers can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase. Consumers can download mobile software applications (“apps”) that can perform a range of consumer services such as locating the nearest retail stores, managing shopping lists, tracking family budgets, or calculating tips or debts. Apps also allow consumers to read news articles, play interactive games and connect with family and friends via

³ ComScore, The 2010 Mobile Year in Review Report (Feb. 14, 2011), *available at* www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_Mobile_Year_in_Review.

⁴ Indeed, a recent industry survey found that 62 percent of marketers used some form of mobile marketing for their brands in 2010 and an additional 26 percent reported their intention to begin doing so in 2011. *See Vast Majority of Marketers Will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011*, ANA Press Release describing the results of a survey conducted by the Association of National Advertisers in partnership with the Mobile Marketing Association, dated January 31, 2011, *available at* www.ana.net/content/show/id/20953.

social media applications. Any of these services can contain advertising, including targeted advertising.

II. FTC's Response to Consumer Protection Issues Involving Mobile Technology

New technology can bring tremendous benefits to consumers, but it also can present new concerns and provide a platform for old frauds to resurface. Mobile technology is no different. Although there are no special laws applicable to mobile marketing that the FTC enforces, the FTC's core consumer protection law – Section 5 of the FTC Act – prohibits unfair or deceptive practices in the mobile arena.⁵ This law applies to marketing in all media, whether traditional print, telephone, television, desktop computer, or mobile device.

For more than a decade, the Commission has explored mobile and wireless issues, starting in 2000 when the agency hosted a two-day workshop studying emerging wireless Internet and data technologies and the privacy, security, and consumer protection issues they raise.⁶ In addition, in November 2006, the Commission held a three-day technology forum that prominently featured mobile issues.⁷ Shortly thereafter, the Commission hosted two Town Hall meetings to explore the use of radio frequency identification (RFID) technology, and its integration into mobile devices as a contactless payment system.⁸ And in 2008, the Commission

⁵ 15 U.S.C. § 45(a).

⁶ FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, available at www.ftc.gov/bcp/workshops/wireless/index.shtml.

⁷ FTC Workshop, *Protecting Consumers in the Next Tech-ade*, available at www.ftc.gov/bcp/workshops/techade. The Staff Report is available at www.ftc.gov/os/2008/03/P064101tech.pdf.

⁸ FTC Workshop, *Pay on the Go: Consumers and Contactless Payment*, available at www.ftc.gov/bcp/workshops/payonthego/index.shtml; FTC Workshop, *Transatlantic RFID*

held a two-day forum examining consumer protection issues in the mobile sphere, including issues relating to ringtones, games, chat services, mobile coupons, and location-based services.⁹

More recently, the agency has invested in new technologies to provide its investigators and attorneys with the necessary tools to monitor and respond to the growth of the mobile marketplace. For example, the Commission has established a mobile technology laboratory, akin to the Commission's longstanding Internet investigative laboratory, containing a variety of smartphones utilizing different platforms and carriers, as well as software and equipment that permit FTC investigators to collect and preserve evidence and conduct research into a wide range of mobile issues, including those related to consumer privacy.

III. Applying the FTC Act to the Mobile Arena

Law enforcement is the Commission's most visible and effective tool for fighting online threats, including those in the mobile marketplace. As described below, the FTC has brought four recent cases that illustrate how Section 5 applies to the mobile arena, including unsolicited text messages and the privacy and security of data collected on mobile devices.

In August 2010, the Commission charged Reverb Communications, Inc., a public relations agency hired to promote video games, with deceptively endorsing mobile gaming applications in the iTunes store.¹⁰ The company allegedly posted positive reviews of gaming apps using account names that gave the impression the reviews had been submitted by

Workshop on Consumer Privacy and Data Security, available at www.ftc.gov/bcp/workshops/transatlantic/index.shtml.

⁹ FTC Workshop, *Beyond Voice: Mapping the Mobile Marketplace*, available at www.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

¹⁰ *Reverb Commc'ns, Inc.*, FTC Docket No. C-4310 (Nov. 22, 2010) (consent order).

disinterested consumers when they were, in actuality, posted by Reverb employees. In addition, the Commission charged that Reverb failed to disclose that it often received a percentage of the sales of each game. The Commission charged that the disguised reviews were deceptive under Section 5, because knowing the connection between the reviewers and the game developers would have been material to consumers reviewing the iTunes posts in deciding whether or not to purchase the games. In settling the allegations, the company agreed to an order prohibiting it from publishing reviews of any products or services unless it discloses a material connection, when one exists, between the company and the product. The *Reverb* settlement demonstrates that the FTC's well-settled truth-in-advertising principles apply to new forms of mobile marketing.

In February, the Commission filed its first law enforcement action against a sender of unsolicited text messages and obtained a temporary restraining order suspending the defendant's challenged operations. The FTC alleged that Philip Flora used 32 pre-paid cell phones to send over 5 million unsolicited text messages – almost a million a week – to the mobile phones of U.S. consumers.¹¹ Many consumers who received Flora's text messages – which typically advertised questionable mortgage loan modification or debt relief services – had to pay a per-message fee each time they received a message. Many others found that Flora's text messages caused them to exceed the number of messages included in their mobile service plans, thereby causing some consumers to incur additional charges on their monthly bill.¹² The Commission

¹¹ *FTC v. Flora*, CV11-00299 (C.D. Cal.) (Compl, filed Feb. 22, 2011).

¹² While the financial injury suffered by any consumer may have been small, the aggregate injury was likely quite large. And, even for those consumers with unlimited messaging plans, Flora's unsolicited messages were harassing and annoying, coming at all hours of the day.

charged Flora with the unfair practice of sending unsolicited text messages and with deceptively claiming an affiliation with the federal government in connection with the loan modification service advertised in the text messages.¹³

The FTC has also taken action against companies that fail to protect the privacy and security of consumer information. Two recent cases highlight the FTC's efforts to challenge deceptive claims that undermine consumers' privacy choices in the mobile marketplace.

First, the Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate a new social network, Google Buzz.¹⁴ The Commission charged that Gmail users' associations with their frequent email contacts became public without the users' consent. As part of the Commission's proposed settlement order, Google must protect the privacy of all of its customers – including mobile users. For example, if Google changes a product or service in a way that makes consumer information more widely available, it must seek affirmative express consent to such a change. This provision applies to *any* data collected from or about consumers, including mobile data. In addition, the order requires Google to implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.

¹³ The complaint against Flora also alleges violations of the CAN-SPAM Act for sending unsolicited commercial email messages advertising his texting services that did not include a valid opt-out mechanism and failed to include a physical postal address. In these emails, Flora offered to send 100,000 text messages for only \$300. See FTC Press Release, *FTC Asks Court to Shut Down Text Messaging Spammer* (Feb. 23, 2011), available at www.ftc.gov/opa/2011/02/loan.shtm.

¹⁴ *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment).

Second, in the Commission’s case against social networking service Twitter, the FTC charged that serious lapses in the company’s data security allowed hackers to obtain unauthorized administrative control of Twitter.¹⁵ As a result, hackers had access to private “tweets” and non-public user information – including users’ mobile phone numbers – and took over user accounts, among them, those of then-President-elect Obama and Rupert Murdoch. The Commission’s order, which applies to Twitter’s collection and use of consumer data, including through mobile devices or applications, prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter’s security practices.

These are just two recent examples of cases involving mobile privacy issues, but the Commission’s enforcement efforts are ongoing.¹⁶ Staff has a number of active investigations into privacy issues associated with mobile devices, including children’s privacy.

IV. Mobile Privacy Policy Initiatives

As noted, the rapid growth of mobile technologies has led to the development of many new business models involving mobile services. On the one hand, these innovations provide valuable benefits to both businesses and consumers. On the other hand, they facilitate unprecedented levels of data collection, which are often invisible to consumers.

The Commission recognizes that mobile technology presents unique and heightened privacy and security concerns. In the complicated mobile ecosystem, a single mobile device can

¹⁵ *Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order).

¹⁶ *See also FTC v. Accusearch, Inc.*, 2007 WL 4356786 (D. Wyo. Sept. 28, 2007) (operation of a website that illegally obtained telephone records, including cell phone records, through pretexting was an unfair act), *aff’d*, 570 F.3d 1187 (10th Cir. 2009).

facilitate data collection and sharing among many entities, including wireless providers, mobile operating system providers, handset manufacturers, application developers, analytics companies, and advertisers. And, unlike other types of technology, mobile devices are typically personal to the user, almost always carried by the user and switched-on.¹⁷ From capturing consumers' precise location to their interactions with email, social networks, and apps, companies can use a mobile device to collect data over time and "reveal[] the habits and patterns that mark the distinction between a day in the life and a way of life."¹⁸ Further, the rush of on-the-go use, coupled with the small screens of most mobile devices, makes it even more unlikely that consumers will read detailed privacy disclosures.

In recent months, news reports have highlighted the virtually ubiquitous data collection by smartphones and their apps. Researchers announced that Apple has been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.¹⁹ The *Wall Street Journal* has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique identifiers associated with a particular mobile

¹⁷ See, e.g., Pew Internet & American Life Project, *Adults, Cell Phones and Texting* at 10 (Sept. 2, 2010), available at www.pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults/Overview.aspx ("65% of adults with cell phones say they have ever slept with their cell phone on or right next to their bed"); *Teens and Mobile Phones* at 73 (Apr. 20, 2010), available at www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones/Chapter-3/Sleeping-with-the-phone-on-or-near-the-bed.aspx (86% of cell-owning teens ages 14 and older have slept with their phones next to them).

¹⁸ *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

¹⁹ See Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, WALL ST. J. (Apr. 21, 2011), available at <http://online.wsj.com/article/SB10001424052748704570704576275323811369758.html>.

device – that can then be used to track and predict consumers’ every move.²⁰ Not surprisingly, recent surveys indicate that consumers are concerned. For example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.²¹

A. Privacy Roundtables

The Commission has been considering these and related issues in connection with its “Exploring Privacy” Roundtable series. In late 2009 and early 2010, the Commission held three roundtables to examine how changes in the marketplace have affected consumer privacy and whether current privacy laws and frameworks have kept pace with these changes.²² During the second roundtable, one panel in particular focused on the privacy implications of mobile technology, addressing the complexity of data collection through mobile devices; the extent and

²⁰ See, e.g., Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J. (Apr. 23, 2011), available at <http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html?mod=> (describing how researchers are using mobile data to predict consumers’ actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, WALL ST. J. (Dec. 18, 2010), available at <http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html?mod=> (documenting the data collection that occurs through many popular smartphone apps).

²¹ NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), available at http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/; see also Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* at 7 (Mar. 2011), available at <http://aa-download.avg.com/filedir/other/Smartphone.pdf> (64% of consumers worry about being tracked when using their smartphones).

²² See FTC, *Exploring Privacy: A Roundtable Series*, available at <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>.

nature of the data collection, particularly with respect to geolocation data; and the adequacy of privacy disclosures on mobile devices.²³

B. Preliminary Staff Privacy Report

Based on the information received through the roundtable process, staff drafted a preliminary report (“Staff Report”) proposing a new privacy framework consisting of three main recommendations, each of which is applicable to mobile technology.²⁴ First, staff recommends that companies should adopt a “privacy by design” approach by building privacy protections into their everyday business practices, such as not collecting or retaining more data than they need to provide a requested service or transaction. Thus, for example, if an app is providing traffic and weather information to a consumer, it does not need to collect call logs or contact lists from the consumer’s device. Further, although the app may need location information, the app developer should carefully consider how long the location information should be retained to provide the requested service.

Second, staff recommends that companies should provide simpler and more streamlined privacy choices to consumers. This means that all companies involved in data collection and sharing through mobile devices – carriers, handset manufacturers, operating system providers, app developers, and advertisers – should work together to provide these choices and to ensure

²³ Transcript of Roundtable Record, *Exploring Privacy: A Roundtable Series* at 238 (Jan. 28, 2010) (Panel 4, “Privacy Implication of Mobile Computing”), available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf.

²⁴ See FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at <http://ftc.gov/os/2010/12/101201privacyreport.pdf>. Commissioners Kovacic and Rosch issued concurring statements available at http://ftc.gov/os/2010/12/101201_privacyreport.pdf at Appendix D and Appendix E, respectively.

that they are understandable and accessible on the small screen. As stated in the Staff Report, companies should also obtain affirmative express consent before collecting or sharing sensitive information such as precise geolocation data.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers, including improving disclosures to consumers about information practices. Again, because of the small size of the device, a key question staff posed in the report is how companies can create effective notices and present them on mobile devices.

After releasing the Staff Report, staff received 452 public comments on its proposed framework, a number of which implicate mobile privacy issues specifically.²⁵ FTC staff is

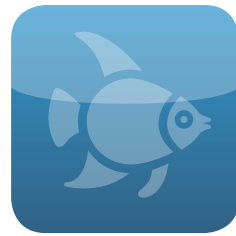
²⁵ See Comment of CTIA (Feb. 18, 2011), *available at* <http://www.ftc.gov/os/comments/privacyreportframework/00375-58002.pdf>; Comment of Verizon and Verizon Wireless (Feb. 18, 2011), *available at* <http://www.ftc.gov/os/comments/privacyreportframework/00428-58044.pdf>; *see also, e.g.*, Comment of Center for Digital Democracy and U.S. PIRG at 10-11, 20-21, 33 (Feb. 18, 2011), *available at* <http://www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf>; Comment of Stanford Security Laboratory at 11-12 (Feb. 18, 2011), *available at* <http://www.ftc.gov/os/comments/privacyreportframework/00467-57980.pdf>.

analyzing the comments and will take them in consideration in preparing a final report for release later this year.²⁶

V. CONCLUSION

The Commission is committed to protecting consumers' privacy in the mobile sphere by bringing enforcement where appropriate and by working with industry and consumer groups to develop workable solutions that protect consumers while allowing innovation in this growing marketplace.

²⁶ Another major initiative addressing the mobile marketplace is the Commission's review of the Children's Online Privacy Protection Rule, issued pursuant to the Children's Online Privacy Protection Act ("COPPA"). Initiated in April 2010, this review sought public comment on whether technological changes to the online environment warrant any changes to the Rule or to the statute. In June 2010, the Commission also held a public roundtable to discuss the implications for COPPA enforcement raised by new technologies, including the rapid expansion of mobile communications. The Rule review is ongoing.



Mobile Apps for Kids:

Current Privacy Disclosures are
Dis *app*ointing



Mobile Apps for Kids:

Current Privacy Disclosures are
Dis *app*ointing

This report is available on the internet at http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
The online version of this report contains live hyperlinks.

Contents

FTC Staff Report.....	1
Overview	1
Recommendations	3
Methodology	4
I. Range of Apps Offered	5
II. Data Collection and Sharing Practices.....	10
Conclusion	17
Endnotes	18
Appendix	AI

FTC Staff Report

Overview¹

The market for mobile applications has experienced explosive growth over the past three and a half years. When Apple's iTunes App Store and Google's Android Market first launched in 2008, smartphone users could choose from about 600 apps.² Today, there are more than 500,000 apps in the Apple App store³ and 380,000 apps in the Android Market,⁴ which consumers can access from a variety of mobile devices, including smartphones and tablets. Consumers have downloaded these apps more than 28 billion times,⁵ and young children and teens are increasingly embracing smartphone technology for entertainment and educational purposes.⁶ As consumers increasingly rely on their mobile devices for multiple activities, the quantity and diversity of mobile apps continue to expand.

This rapidly growing market provides enormous opportunities and benefits for app users of all ages, but raises questions about users' privacy, especially when the users are children and teens. Mobile apps can capture a broad range of user information from the device automatically – including the user's precise geolocation, phone number, list of contacts, call logs, unique device identifiers, and other information stored on the mobile device – and can share this data with a large number of possible recipients. These capabilities can provide beneficial services to consumers – for example, access to maps and directions, and the ability to play interactive games with other users – but they also can be used by apps to collect detailed personal information in a manner parents cannot detect.

Protecting children's privacy is one of the Commission's top priorities. In order to better understand and evaluate the emerging app market and the products and services it offers to children, Federal Trade Commission staff designed and conducted a survey of the apps offered for children in the two largest U.S. app stores, the Android Market and the Apple App store. Staff focused in particular on the types of apps offered to children; the age range of the intended audience; the disclosures provided to users about the apps' data collection and sharing practices; the availability of interactive features, such as connecting with social media; and the app store ratings and parental controls offered for these systems. This report highlights the lack of information available to parents prior to downloading mobile apps for their children, and calls on industry to provide greater transparency about their data practices.⁷

Staff searched the app stores using the word “kids,” and examined hundreds of pages promoting apps, which ranged from alphabet and word games, math and number games, and memory games to books and stories, flash cards, and puzzles. Most of the apps’ descriptions specifically indicated that the apps were intended for use by children, and some promoted use by children of certain ages, stating, for example, “teach young children, ages 2 to 5.” Prices ranged from free to \$9.99, but most apps were \$0.99 or less, and free apps were overwhelmingly the most frequently downloaded.

While staff encountered a diverse pool of apps for kids created by hundreds of different developers, staff found little, if any, information in the app marketplaces about the data collection and sharing practices of these apps. Staff found almost no relevant language regarding app data collection or sharing on the Apple app promotion pages,⁸ and minimal information (beyond the general “permission” statements required on the Android operating system⁹) on just three of the Android promotion pages. In most instances, staff was unable to determine from the promotion pages whether the apps collected any data at all, let alone the type of data collected, the purpose of the collection, and who collected or obtained access to the data.

As part of its mission to protect children, the Commission vigorously enforces the Children’s Online Privacy Protection Act (“COPPA”) and the FTC’s implementing Rule, which require operators of online services (including interactive mobile apps) directed to children under age 13 to provide notice and obtain parental consent before collecting items of “personal information” from children.¹⁰ Since collecting the data for this survey, the FTC settled its first COPPA enforcement action against a mobile app developer¹¹ and issued a Notice of Proposed Rulemaking to amend the Commission’s COPPA Rule.¹² Those initiatives, along with this report, are a warning call to industry that it must do more to provide parents with easily accessible, basic information about the mobile apps that their children use.

Most of the apps in the study appear to be intended for children’s use, and many may, in fact, be “directed to children” within the meaning of COPPA.¹³ This survey focused on the disclosures provided to users regarding their data practices; it did not test whether the selected apps actually collected, used, or disclosed personal information from children. Over the next six months, staff will conduct an additional review to determine whether there are COPPA violations and whether enforcement is appropriate.¹⁴ Staff also will evaluate whether the industry is moving forward to address the disclosure issues raised in this report.

Recommendations

FTC staff believes that all members of the kids app ecosystem – the app stores, developers, and third parties providing services within the apps – should play an active role in providing key information to parents who download apps. The mobile app marketplace is growing at a tremendous speed, and many consumer protections, including privacy and privacy disclosures, have not kept pace with this development. Parents need easy access to basic information so they can make informed decisions about the apps they allow their children to use.¹⁵

App developers should provide this information through simple and short disclosures or icons that are easy to find and understand on the small screen of a mobile device. Parents should be able to learn what information an app collects, how the information will be used, and with whom the information will be shared.¹⁶ App developers also should alert parents if the app connects with any social media, or allows targeted advertising to occur through the app. Third parties that collect user information through apps also should disclose their privacy practices, whether through a link on the app promotion page, the developers' disclosures, or another easily accessible method.

The app stores also should do more to help parents and kids. The two major app stores provide the basic architecture for communicating information about the kids apps they offer, such as pricing and category information. However, the app stores should provide a more consistent way for developers to display information regarding their app's data collection practices and interactive features. For example, app stores could provide a designated space for developers to disclose this information. The app stores also could provide standardized icons to signal features, such as a connection with social media services. Although the app store developer agreements require developers to disclose the information their apps collect, the app stores do not appear to enforce these requirements.¹⁷ This lack of enforcement provides little incentive to app developers to provide such disclosures and leaves parents without the information they need. As gatekeepers of the app marketplace, the app stores should do more. This recommendation applies not just to Apple and Google, but also to other companies that provide a marketplace for kids mobile apps.

Additional work is needed to identify the best means and place for conveying data practices in plain language and in easily accessible ways on the small screens of mobile devices. Staff encourages industry members, privacy groups, academics, and others to develop and test new ways to provide information to parents – for example, by standardizing language,

creating icons, or using a layered approach. To this end, the Commission currently is engaged in a project to update its existing business guidance, “Dot Com Disclosures,” about online advertising disclosures.¹⁸ As part of this project, the agency will host a public workshop in 2012 to gain input from interested parties, including industry representatives, consumer groups, and consumer disclosure experts. One of the topics that will be addressed is mobile privacy disclosures, including how they can be short, effective, and accessible to consumers on small screens. Staff anticipates that the workshop discussion will spur further development in this area.

Methodology

In July 2011, FTC staff searched on the desktop version of Apple’s App Store and the browser-based version of the Android Market for the term “kids.”¹⁹ The search yielded over 8,000 results in the Apple App Store and over 3,600 in the Android Market. Staff collected the app promotion pages for the first 480 results returned by each app store,²⁰ for a total of 960 apps. Both app stores provide a promotion page for each app offered, which typically lists the name of the app developer directly under the app title and includes a textual description of the app. The app promotion page also displays information such as the app’s price, publication date, app store category, content maturity rating, user feedback ratings, number of user feedback ratings, screenshot previews, developer contact information, and, in many instances, a link to a developer website.²¹

Staff then conducted a closer review of the promotion pages for 200 Android apps and 200 Apple apps chosen randomly from each pool of the 480 “kids” results. Staff examined the information listed on the app store promotion page and the first page (“landing” page) of the associated developer’s website. On the app store promotion page, staff looked for language and terms in the app description in order to sort the apps by type and intended audience. Staff also looked to see if the app linked to any social media, allowed users to make purchases (“in-app” purchases), included advertising, displayed developer contact information, and provided information about the app’s data collection practices. On the landing page of the developer website, staff looked for additional information about the app, as well as contact and data collection information for the developer.²²

Staff notes two additional points with respect to the methodology. First, staff did not download any of the apps surveyed, and did not test the apps’ information collection, use, or disclosure practices. Rather, staff reviewed the information that a consumer easily could access either from the app store or from the developer’s website prior to downloading the app.

Information provided to parents after downloading an app is, in staff’s view, less useful in the parent’s decision-making since, by then, the child may already be using the app and the parent already could have been charged a fee.²³

Second, staff reviewed only the app store pages made available to desktop computer visitors, which allowed staff to electronically collect and preserve the app promotion pages at a specific moment in time. Staff recognizes that there are a few differences between the content offered through the desktop interface and the content offered through the mobile device interface, but does not believe these differences are material or change the conclusions of this report.²⁴

I. Range of Apps Offered

Staff found a wide range of kids apps offered at low prices by hundreds of developers.

Types of Apps for Kids

To get a sense of the types of apps available for kids, staff categorized each of the 400 apps based on language contained in the app name or description.²⁵ For example, a multiplication flash card app would fall into the “educational,” “math,” and “flash cards” categories. Staff found that education, games, math, spelling, and animals were the most popular app categories. The percentage of apps found by subject category is listed in Table 1.

Table 1: Categories of “Kids” Apps

Category	Apple App Store	Android Market
	% of Apps	% of Apps
Educational	51.0%	50.0%
Game	49.5%	41.0%
Animal-related	22.0%	23.0%
Alphabet/Spelling/Words	20.5%	17.0%
Math/Numbers	20.0%	16.5%
Matching	16.0%	9.5%
Memory	14.0%	15.5%
Book/Story	12.5%	6.5%
Coloring	9.0%	17.0%
Musical	7.0%	6.0%
Puzzle	6.5%	8.0%
Learning a language	6.5%	11.0%
Flash Cards	3.5%	3.5%
Photo-related	2.5%	4.0%
Quiz/Test	1.5%	3.5%
Jokes	1.0%	1.0%
Other ²⁶	8.5%	14.5%
	n=200	n=200

Intended Audience

Staff also reviewed the app descriptions for cues to the intended audience, looking for both general and specific age groups. Almost all of the apps reviewed appeared to be intended for use by kids, and many provided specific age ranges. Staff looked for words in app names or descriptions suggesting that the apps were recommended for, or were appropriate for, certain general groups, such as “infants,” “toddlers,” “preschoolers,” “children,” “kids,” “parents” and “teachers.”²⁷ Table 2 lists the percentage of apps on each platform promoted for use by certain age groups.

Table 2: Intended Audience – General Age Groups

General Age Group	Apple App Store % of Apps	Android Market % of Apps	Combined % of Apps
Infant/Toddler	11.5%	4.0%	
Child	56.0%	40.5%	
Kid	63.5%	76.5%	89.75%
Preschool	7.5%	10.5%	
Elementary School	1.5%	1.5%	
Parent	17.5%	20.0%	
Teacher	3.5%	2.5%	24.25%
Adult	7.5%	2.5%	
Family	6.0%	4.5%	5.25%
Everyone	5.0%	1.0%	3.00%
No Indication	8.0%	2.0%	5.00%
	n=200	n=200	n=400

Most of the app promotion pages suggested that the apps were for kids (or some subset of kids, such as infants) as shown in Table 2. Twenty-four percent of the 400 app descriptions contained language suggesting that the apps were intended for use by an adult, such as a parent or teacher, but most of those apps indicated they were for use by kids too. While 5% (twenty) of the 400 app descriptions did not include language suggesting any intended audience, all but two of these apps appeared to include content that kids may enjoy, such as games like checkers, table tennis, and basketball. Overall, staff estimates that about 95% of the 400 apps reviewed in detail were apps intended for kids’ use.²⁸

Twenty three percent of the 400 apps specified a particular age range or school grade level. For these apps, staff recorded the recommended age ranges, converting any grade levels to ages.²⁹ Over 50% of the apps that listed an age or grade range listed a range beginning at 2 years old or younger; over 80% listed a range beginning at age four or younger; and over 90%

specified an age range starting at 6 years old or younger.³⁰ Conversely, over 75% of the apps that specified an age range specified one ending at 12 years old or younger, and roughly 45% specified an age range ending at 6 years old or younger. Table 3 lists the number of apps for specified age ranges.

Table 3: Intended Audience – Specific Age Ranges

		Maximum recommended age					% of apps with this min. age
		3-4	5-6	7-8	9-12	13+	
Minimum recommended age	0-2	9	27	6	2	11	60%
	3-4		1	8	5	9	25%
	5-6		4	1	1	1	8%
	7-8			3	2		5%
	13					1	1%
% of apps with this max. age		10%	35%	20%	11%	24%	n=91

Most Kids Apps Are Inexpensive

While prices ranged from free to \$9.99, most of the 960 app store promotion pages listed a price of \$0.99 or less. Indeed, 77% of the apps in the survey listed an install price of \$0.99 or less, and 48% were free.³¹ Free apps appeared to be the most frequently downloaded.

The Android Market provides a “download range” and a “feedback” field on the promotion page of each app. The “download range” is an estimate of the number of times a particular app has been downloaded (such as “100 – 500” or “10,000 – 50,000”) while the “feedback” field reveals the number of app users that have provided comments or feedback regarding their experience with the app. Staff used the download ranges to estimate the relative popularity of apps in each price category.³² Using this indicator, staff found that the free Android apps accounted for 99% of all downloads in the Android survey results, even though they accounted for only 62% of the apps returned by the “kids” search. Staff then compared these findings to the results obtained by using the “feedback” information to infer app popularity. As shown in Table 4, the “feedback” method closely tracked the “download” method.

Table 4: Android Market Price and Popularity

Price	% of Apps	% of Downloads ³³	% of Feedback Ratings
Free	61.7%	99.43%	97.64%
\$0.01 to \$0.99	14.0%	0.13%	0.19%
\$1 to \$1.99	9.2%	0.09%	0.27%
\$2 to \$2.99	2.9%	0.23%	1.43%
\$3 to \$3.99	1.6%	0.09%	0.37%
\$4.00+	1.6%	0.01%	0.03%
Foreign	9.0%	0.02%	0.07%

n=480

Apple’s App Store does not provide download ranges for its apps, but it does display the number of users that have provided feedback for each app. As with Android, staff used the number of feedback ratings to infer the relative popularity of the Apple apps. Staff found that free Apple apps appeared to be more popular than paid apps, accounting for 68% of all “ratings,” even though they only accounted for 35% of the search results (see Table 5).

Table 5: Apple App Store Prices and Popularity

Price	% of Apps	% of Ratings
Free	34.80%	68.29%
\$0.99	43.95%	22.08%
\$1.99	14.58%	9.15%
\$2.99	3.75%	0.19%
\$3.99	1.04%	0.10%
\$4.99	1.88%	0.19%

n=480

Number of Developers

Staff found that hundreds of developers were responsible for the apps in the study. Staff encountered 441 unique developers in this study, only twelve of which had apps on both platforms. Table 6 presents the number of developers responsible for the apps in the search results.

Table 6: Number of Apps Per Developer and Popularity Indicators

# of Apps Per Developer	Apple App Store			Android Market		
	# of Developers	% All Apps	% Feedback Ratings	# of Developers	% All Apps	% of Downloads
1	142	29.6%	49.8%	150	31.3%	50.2%
2	43	17.9%	18.8%	48	20.0%	9.7%
3	11	6.9%	6.0%	11	6.9%	2.2%
4	5	4.2%	4.4%	6	5.0%	9.1%
5-9	13	17.7%	19.8%	14	16.9%	7.3%
10+	5	23.8%	1.1%	5	20.0%	21.4%
	n=480			n=480		

Only a handful of app developers were responsible for more than 10 apps in our sample. Developers with one app in our sample were popular, accounting for about 50% of all downloads/feedback ratings, even though they were responsible for only about 30% of the apps. In contrast, those developers with more than 10 apps in our sample accounted for about 1% of the feedback ratings for Apple, (and 20% of the downloads for Android) despite accounting for about 20% of all of the apps in the survey. This finding illustrates the broad and diverse nature of the mobile app marketplace.

Contact Information

Many of the developers provided some type of contact information directly on their app’s promotion page, or linked to a developer website that contained contact information. Staff found that 13% of the 400 kids apps listed an email address somewhere on the promotion page.³⁴ Eighty-one percent of the 400 app promotion pages linked to a functioning English-language developer website, a number of which provided contact information.³⁵ Sixty-five percent (of the 400) linked to a functioning developer website whose landing page contained either some form of contact information or a link to contact information.³⁶ Within this group, 23% (of the 400) linked to a developer website that listed an email address on the landing page, 8% linked to a landing page providing a phone number, 6% linked to a landing page with a mailing address, 2% provided all three types of contact information on the landing page, and 38% linked to a landing page containing a link that appeared to lead to contact information.³⁷

II. Data Collection and Sharing Practices

The survey findings regarding data collection and sharing were of greatest concern to FTC staff. Indeed, across the wide range of “kids” apps examined in the survey, staff found very little information about the data collection or sharing practices of these apps. Apple’s and Google’s mobile operating systems and app stores provide limited notice to users regarding app capabilities, and leave the bulk of disclosure to individual app developers. In most instances, staff was unable to determine from the information on the app store page or the developer’s landing page whether an app collected *any* data, let alone the type of data collected, the purpose for such collection, and who collected or obtained access to such data.³⁸ This is troubling given the ability of mobile apps to access users’ information on devices automatically and to transmit this information invisibly to a wide variety of entities.

The Mobile App Stores and Operating Systems

Apple’s iOS and Google’s Android operating systems offer powerful capabilities to the mobile applications that run on them.³⁹ For example, they enable mobile apps to determine the user’s precise geolocation and communicate with other devices via the Internet. For mobile gaming apps, these systems may allow a child to identify and connect with others playing the same game nearby. The operating systems also may provide apps with access to sensitive information such as a user’s call logs, contacts, and unique device identifiers, or enable the app to use the phone service on the mobile device to make or answer calls or send text messages. Depending on the type of service the app provides and how the app has been configured, this broad access to data may or may not be necessary to provide the service and may occur without the user’s knowledge.

The app stores and operating systems take different approaches to managing the information and capabilities that apps may access. Android requires its apps to declare any potentially sensitive capabilities on a “permissions” screen, which displays just before installing the app.⁴⁰ While helpful, these disclosures do not explain clearly (or provide an easy means for consumers to learn) why an app has the permissions it does, what the app does with such access, or whether the app shares any information with third parties. Providing clear and accessible information is especially important in the kids app space, where any data accessed and collected would likely be from a mobile device used by a child, and could reveal information that a parent may not want shared with unknown third parties, such as a child’s precise geolocation or phone number. Faced with concerns about what data an app may or may not collect, a parent may be forced to choose between downloading the app, and running

the risk that the child’s sensitive information will be shared with unknown third parties, or not downloading the app, and depriving the child of an enjoyable game or activity.

Of the 182 Android apps indicating they were intended for use by kids, only 24% specified that the app required “no special permissions to run” – *i.e.*, that a child could use the app without the app accessing any information or capabilities from the mobile device. Conversely, 76% indicated that the app required at least one “permission” to run. In fact, staff found that over half of the Android app promotion pages listed a “permission” for “full Internet access,” meaning that the “permission” enables the app to access and receive a wide variety of content while the app is running.⁴¹ Table 7 lists the percentage of Android apps that contained some of the more potentially sensitive permissions.⁴²

Table 7: Android Market “Kids” Apps Permissions

Permission	% of Apps	% of Free Apps	% of Paid Apps
Network communication: full Internet access	60.99%	78.81%	28.13%
Phone calls: read phone state and identity ⁴³	20.88%	29.66%	4.69%
Modify/delete SD card ⁴⁴	15.93%	16.95%	14.06%
Your location -	8.24%	11.02%	3.13%
Fine (GPS) location	6.04%	7.63%	3.13%
Coarse (network-based) location	5.49%	7.63%	1.56%
Both fine and coarse location	3.30%	4.24%	1.56%
Hardware controls: take pictures and videos	3.85%	4.24%	3.13%
Services that cost you money: directly call phone numbers	2.20%	3.39%	0.00%
Modify global system settings	2.75%	3.39%	1.56%
Hardware controls: record audio	1.65%	2.54%	0.00%
Your personal information: read sensitive log data	0.55%	0.85%	0.00%
No special permissions	24.18%	13.56%	43.75%
	n=182	n=118	n=64

In contrast to Android’s “permissions” approach, Apple states that it relies on an app review process in which it screens and approves apps before permitting them to be offered in Apple’s app store.⁴⁵ Because Apple’s App Store does not require its apps to display “permissions” to users prior to download, staff could not measure the degree to which the Apple kids apps were capable of accessing device information.⁴⁶ Apple states that it reviews every application “in order to protect consumer privacy” and “safeguard children from inappropriate content,”⁴⁷ and that “any App that targets minors for data collection will be rejected.”⁴⁸ The details of this screening process are not clear.

Location information is treated differently from other information by each system but follows essentially an “on/off” model. Both operating systems can signal the user when an

app requests the user's location by displaying a specific icon.⁴⁹ Both systems also provide a global setting that allows users to turn off their devices' location capabilities.⁵⁰ As described above, Android's operating system requires developers to declare a "permission" for access to location information. After an app is downloaded, Apple's operating system provides: 1) a notice the first time that an app attempts to acquire the user's location; and 2) an on/off switch in the device's settings allowing users to permit an app to access their location information on an app-by-app basis.⁵¹ These additional protections offered by Apple apply only to an app requesting location information.

Beyond the basic technological models, both app stores require developers by agreement to disclose the information their apps collect,⁵² though neither store specifies how or where such information should be provided. Both stores' privacy policies also state that the privacy policies of the app developers control the practices of a mobile app offered in the app stores.⁵³ Under this model, the information provided by developers is critical for transparency. Nevertheless, as described below, such information is rarely provided.

Disclosure of App Data Collection and Sharing

Staff's review of both the app store promotion pages and developer websites of the 400 closely examined apps in the survey revealed very little information about the apps' data practices.

Indeed, the Apple app promotion pages that staff examined provided almost no information on individual developers' data collection and sharing practices. Similarly, the Android app promotion pages that staff examined provided little information other than the mandatory "permissions." Only three (1.5%) of the 200 Android apps even attempted to convey information about the purpose for the "permissions." These three apps made the following disclosures (respectively) on their promotion pages:

- "Needs Location permission for Ads. If you prefer, get the AD FREE version."
- "Permissions are required by the Ad networks, which keep the app free."
- "All requested permissions are for ads only."

All three statements put the user on notice that the app provides information to an ad network, but do not identify what information is collected, by whom, how it is used, and whether it is shared with others.

Staff also looked for information about the apps' data collection and sharing practices on the landing pages of the developers' websites.⁵⁴ As with the app promotion pages, staff

found very little information. Sixteen percent of the 400 kids app promotion pages linked to a developer landing page that contained or linked to disclosure information. Within this group, 13% (of the 400) linked to a landing page that displayed a link labeled “privacy policy,” and the remaining 3% linked to developer sites that provided links to some other disclosures. These other disclosures had labels such as “terms of use,” “terms and conditions,” “terms of service,” “Legal Notices,” and “disclaimers.”⁵⁵ Out of the entire set of 400 app promotion pages examined, only two (0.5%) linked to a developer landing page that disclosed information about data collection and sharing on the landing page itself.

Disclosure of Additional Interactive Features

Staff also examined the app store promotion pages for features that may serve as a platform for data collection, such as the ability to make purchases within the app, connect with social media, and serve targeted advertising. These features often are provided to the app developer by various third parties, who may gain access to kids’ data as a result.

In-App Purchase Mechanism

Some developers offer app users the ability to purchase additional content via an in-app purchase mechanism. For example, a storybook application may come with a single story, but then allow the app user to purchase additional stories without having to leave the app. The ability of children to purchase items within mobile applications has been a subject of concern in media reports and by members of Congress, as parents may not know about such capabilities prior to download.⁵⁶

Staff found that 11.0% of the 200 Apple App Store promotion pages, and 0.5% of the 200 Android pages indicated that the app had some form of in-app purchase mechanism. While Apple includes a box disclosing “Top In-App Purchases” on the promotion page for apps with in-app purchase mechanisms, Android appears to require only those developers that use Android’s own in-app purchasing mechanism to display a permission discussed above.⁵⁷ In light of the significant concerns raised by in-app purchase capabilities in apps for children, staff is evaluating what types of protections should apply to these capabilities. It is clear, however, that confusing and hard-to-find disclosures do not give parents the control that they need in this area.

Staff believes that parents need consistent, easily accessible, and recognizable disclosures regarding in-app purchase capabilities so that they can make informed decisions about whether to allow their children to use apps with such capabilities.

Social Network Integration and Other Social Features

Staff found that 5% of the 400 app promotion pages indicated that the app was integrated with a social network – that is, a user could access a social network, and thus share information, through the app. Staff found that 3.5% of the 400 promotion pages indicated integration with Facebook, 2% with Twitter, and 2% with various other social networks.⁵⁸ Because the app stores do not appear to require disclosure of these social features on the promotion page, it is likely that the survey numbers understate the prevalence of social functionality. In addition, some apps have their own internal sharing functions – for example, automatically sharing game results, usernames, and other information with unknown users on the app’s scoreboard or news feed. Staff believes that the presence of social features within an app is highly relevant to parents selecting apps for their children, and that such functionality should be disclosed prior to download.

In-App Advertising

The existence of advertising within an app may be significant to parents for several reasons. First, parents may want to limit the data collected by advertisers and ad networks about their children.⁵⁹ Second, even if the advertising is not based on any information collected by the user, parents may want to limit their children’s exposure to ads. Finally, ads running inside an app may incorporate various capabilities allowing the user to do things like directly call phone numbers or visit websites appearing in the ad, and parents may not want these options available to their children.

Staff found that about 7% of the 400 app store promotion pages indicated that the app contained advertising. As above, this number is likely to understate the number of apps containing advertising because app stores do not appear to require developers to disclose in-app advertising on their promotion pages, and because advertising is a common way to monetize apps.⁶⁰ Some of the disclosures appeared to be designed to warn parents about the potential exposure of their children to ads. For example, one promotion page indicated that the app would only display ads during the initial download, when parents would be the likely audience. Other statements attempted to address the information collection aspect of targeted in-app advertising. As previously discussed, three of the Android apps attempted to explain (though fairly cryptically) that a permission to access certain information was related to in-app advertising.

Still others included language addressing the “click-to” functionality often found within advertisements – for example, stating that the developer had moved the placement of banner ads to the top of the screen within the app in order “to avoid accidental clicks by the little fingers.” Some app developers appeared to be offering certain protections to users as a selling-point in the competitive app market. For example, several app promotion pages included language indicating that the app was “ad free,” and one disclosed that, “[f]or security reasons,” the app switched the device to “airplane mode” when in use in order to “protect you [sic] children from any risk.”

The presence of these statements to parents and other users suggests that certain developers are aware of parents’ concerns and are taking some steps to respond. However, parents need clear, easy-to-read, and consistent disclosures regarding the advertising that their children may view on apps, especially when that advertising is personalized based on the child’s in-app activities. And to the extent that third parties providing the advertising (or other interactive features) gain access to kids’ data in providing these services, they also must ensure that their data practices are disclosed to parents in a clear and meaningful way.

App Rating Systems and Parental Controls

Both app stores and operating systems offer rating systems and controls that can provide parents with useful tools to manage their children’s access to and use of mobile apps. The systems allow parents to restrict access to mobile content and features, and can limit the collection of data from the mobile device, such as limiting the sharing of geolocation information. These systems are not designed, however, to provide specific information about the data collected and shared by apps.⁶¹

Rating Systems⁶²

The Apple App Store and the Android Market assign various content ratings to the apps they offer indicating a recommended level of maturity. Some of the parent controls rely on these content ratings to screen out inappropriate material.⁶³ Apple’s and Android’s content ratings are unique to the particular app store, and the methods for evaluating content and assigning ratings rely largely on the app developer to supply the initial rating.⁶⁴

Apple’s content ratings consist of four different age indicators (“4+,” “9+,” “12+,” and “17+”) that are assigned to apps as part of Apple’s approval process. Prior to submitting an app to Apple for approval, app developers must fill out a ratings matrix.⁶⁵ The matrix requires the developer to select the frequency (e.g., “none,” “infrequent/mild,” or “frequent/

intense”) of different types of content (“Cartoon or Fantasy Violence,” “Sexual Content or Nudity,” “Profanity or Crude Humor,” etc.), and assigns a rating based on the developer’s input.⁶⁶ Staff did not evaluate the appropriateness of any of the ratings assigned, but notes that nearly all of the Apple apps reviewed in this survey contained the lowest content rating of “4+.” See Table 8.

Table 8: Content Ratings for Apple App Store “Kids” Apps

Apple Content Rating	Apple App Store
“4+”	97.5%
“9+”	1.5%
“12+”	1.0%
“17+”	0%
	n=200

Content ratings in the Android Market also are largely determined by the app developer, and consist of four different maturity indicators (“Everyone,” “Low maturity,” “Medium maturity,” and “High maturity”).⁶⁷ Android’s ratings do not map directly to specific ages but, like Apple’s, are tied to violent or mature content. Android provides content-based guidelines to developers, and requires that maturity ratings be tied to the app’s functionality.⁶⁸ For example, the guidelines state that “Apps rated ‘Everyone’ must not ask users for their location.”⁶⁹ As shown in Table 9, an overwhelming majority of the Android apps reviewed by staff contained the lowest content rating of “Everyone.” A number of the Android apps involved in this survey did not contain a maturity rating because they pre-dated Android’s introduction of the content rating requirement in November 2010. Twenty-two such apps appeared in staff’s review and are not included in the percentages presented in Table 9.

Table 9: Content Ratings for Android Market “Kids” Apps⁷⁰

Android Content Rating	Android Market
“Everyone”	83%
“Low maturity”	12%
“Medium maturity”	2%
“High maturity”	2%
	n=178

Parental Controls

Both app stores provide various controls allowing parents to restrict which apps may be downloaded onto their children’s mobile devices, based on app content ratings.⁷¹ In addition, Apple’s mobile operating system incorporates controls that allow parents to password-protect

access to a number of specific applications, such as Apple’s Internet browser (Safari), the online video website YouTube, the iTunes App Store itself, the device’s camera application, as well as some device capabilities, such as location sharing and in-app purchase mechanisms.⁷² Although the Android operating system does not have such built-in parental controls, a number of available apps allow parents to password-protect access to various content and device capabilities.⁷³

On both systems, parents can set the device settings to limit the flow of some information – for example, blocking GPS location sharing or setting the device on “airplane mode” in order to restrict the interactive features of an app. However, a parent needs to set these limits each time the child uses an app, and taking such actions may adversely limit desirable app functionality.⁷⁴ Further, while these types of controls may help parents manage the use of the device by their children, they do not provide information about the data practices associated with the apps that run on them. Thus, parents may be forced to choose between allowing their child to use an app, with all the unknown risks associated with such use, and cutting off their child’s use of the app altogether. With better information about the data practices of these apps, parents can make informed decisions about which apps their children can use safely, and which apps parents wish to avoid.

Conclusion

The mobile apps marketplace is a constantly evolving new media that offers parents many new options for entertaining and educating their children. Staff’s survey shows, however, that parents generally cannot determine, before downloading an app, whether the app poses risks related to the collection, use, and sharing of their children’s personal information. Although the two major U.S. mobile app stores provide some information and controls governing apps, all members of the mobile app ecosystem – the app stores, the developers, and the third parties providing services within the apps – must do more to ensure that parents have access to clear, concise and timely information about the apps they download for their children. Parents should be able to learn, before downloading an app for their children, what data will be collected, how the data will be used, and who will obtain access to the data. Armed with such information, parents can make knowledgeable decisions about the apps they choose for their children, and embrace these technologies with more confidence. Staff is committed to working with all stakeholders on these issues, and also plans to continue its vigorous enforcement of the COPPA statute and Rule. Staff hopes that this report will spur greater transparency and meaningful disclosure about the data collection practices in apps for children.

Endnotes

1. The primary authors of this FTC staff survey and report are Patricia Poss and Andrew Hasty of the FTC's Bureau of Consumer Protection. They received valuable assistance from Andrew Bristow, a Princeton student on temporary staff at the FTC, and staff from throughout the Bureau of Consumer Protection. Robert Letzler and Michael Shores of the Bureau of Economics provided valuable assistance with presentation of the empirical results.
2. Apple offered 552 apps at launch in July 2008. Michael Arrington, *iPhone App Store Has Launched (Updated)*, TechCrunch (July 10, 2008), <http://techcrunch.com/2008/07/10/app-store-launches-upgrade-itunes-now/>. Google's Android Market offered 50 apps when it launched in October 2008. Dean Takahashi, *Google Releases Details on Android Market Launch*, VentureBeat (Oct. 22, 2008), <http://venturebeat.com/2008/10/22/google-releases-details-on-android-market-launch/>.
3. Press Release, Apple, *Apple's Mac App Store Downloads Top 100 Million* (Dec. 12, 2011), <http://www.apple.com/pr/library/2011/12/12Apples-Mac-App-Store-Downloads-Top-100-Million.html>.
4. *Google Android Market*, Distimo, http://www.distimo.com/appstores/app-store/19-Google_Android_Market (last updated Dec. 30, 2011).
5. See Press Release, Apple, *Apple's Mac App Store*, *supra* note 3 (more than 18 billion downloads from Apple App Store); Eric Chu, *10 Billion Android Market Downloads and Counting* (Dec. 6, 2011), <http://android-developers.blogspot.com/2011/12/10-billion-android-market-downloads-and.html>.
6. Common Sense Media reported that half (52%) of all children in the United States have access to a smartphone (41%), a video iPod (21%), or an iPad or other tablet device (8%). Common Sense Media, *Zero to Eight: Children's Media Use in America 9* (Fall 2011), available at www.commonsensemedia.org/sites/default/files/research/zerotoeightfinal2011.pdf. Another study indicated that two-thirds of the children ages 4-7 stated they had used an iPhone, often one owned by a family member and handed back to them while riding in an automobile. Cynthia Chiong & Carly Shuler, Joan Ganz Cooney Center, *Learning: Is there an App for that?* 15 (Nov. 2010), available at www.joanganzcooneycenter.org/upload_kits/learningapps_final_110410.pdf. In addition, recent research states that "In the third quarter of 2011, teens age 13-17 used an average of 320 MB of data per month on their phones, increasing 256 percent over last year and growing at a rate faster than any other age group." *New Mobile Obsession: U.S. Teens Triple Data Usage*, Nielsen (Dec. 15, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/new-mobile-obsession-u-s-teens-triple-data-usage/.
7. These recommendations are consistent with the FTC staff's preliminary privacy report that called on companies to be more transparent as to their data collection practices and encouraged companies to offer short, easy-to-read disclosures (or icons) that consumers are likely to see, read, and understand. See FTC Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* 69-71 (Dec. 1, 2010), available at <http://ftc.gov/os/2010/12/101201privacyreport.pdf>.
8. A promotion page is the screen in the app store where a developer provides certain basic information about its app.
9. As discussed further below, "permissions" are phrases describing an app's capabilities that appear on the mobile screen prior to downloading an app in the Android app store.
10. The Commission's COPPA Rule was promulgated pursuant to the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506. The text of the COPPA Rule can be found at 16 C.F.R. Part 312.
11. *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011) (FTC consent order with developer of child-directed mobile apps for alleged violations of the COPPA Rule), available at <http://ftc.gov/os/caselist/1023251/110908w3order.pdf>.
12. Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (proposed Sept. 27, 2011) (stating that "online services" currently covered by the COPPA Rule "includes mobile applications that allow children to play network-connected games, engage in social networking activities, purchase goods or services online,

- receive behaviorally targeted advertisements, or interact with other content or services.”), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf>.
13. See 16 C.F.R. § 312.2 (defining “[w]ebsite or online service directed to children”).
 14. FTC investigations are nonpublic until the Commission takes a public action such as issuing a complaint or announcing a settlement.
 15. A number of organizations have issued guidance for app developers. See Press Release, Future of Privacy Forum, *FPF and CDT Release Best Practices for Mobile Apps Developers* (Dec. 21, 2011), <http://www.applicationprivacy.org/?p=1947>; Press Release, Mobile Marketing Association, *Mobile Marketing Association Releases New Privacy Policy Guidelines for Mobile Apps for Public Comment* (Oct. 17, 2011), <http://mmaglobal.com/news/mobile-marketing-association-releases-new-privacy-policy-guidelines-mobile-apps-public-comment>; Privacy Choice, *PrivacyChoice Challenges Developers to “Get Their Apps in Gear”* (Oct. 18, 2011), *available at* <http://blog.privacychoice.org/2011/10/18/get-your-apps-in-gear/>.
 16. If the app is directed to children and in fact collects information from children, the app must provide a notice and obtain parental consent prior to collection pursuant to COPPA. See 16 C.F.R. § 312.3. In addition, Commission staff has stated more generally that when companies collect sensitive information about children and precise geolocation data, companies should seek affirmative express consent before the data is collected or shared. See FTC Preliminary Staff Report, *supra* note 7, at 61.
 17. See *Best Practices for Mobile Applications Developers*, Future of Privacy Forum, 3, <http://www.futureofprivacy.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf> (last visited Jan. 24, 2012) (citing section 3.3.10 of the iOS Developer Program License Agreement, stating that “Developers must provide clear and complete information to users regarding collection, use and disclosure of user or device data.”); Android Market Developer Distribution Agreement, 4.3, <http://www.android.com/us/developer-distribution-agreement.html> (last visited Oct. 31, 2011) (“If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your Product, and you must provide legally adequate privacy notice and protection for those users.”); see also Scott Thurm & Yukari Iwatani Kane, *Your Apps are Watching You*, Wall St. J., Dec. 18, 2010, *available at* <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html> (reporting that numerous Apple and Android applications transmitted user information, and numerous apps did not provide privacy policies on their websites or inside the apps at the time of testing).
 18. See Press Release, FTC, *FTC Seeks Input to Revising its Guidance to Business About Disclosures in Online Advertising* (May 26, 2011), *available at* <http://www.ftc.gov/opa/2011/05/dotcom.shtm>.
 19. The report focuses on the information available to parents selecting apps for children, who would in most instances be under 13 years of age. Parents of teens, however, may have similar concerns about the collection of information from apps their older children use.
 20. Staff does not know what factors the app stores use to determine the rank order of the apps returned from their search functions. The apps appeared relevant to the search term “kids.”
 21. The Android Market also provides an estimated range of the number of times an app has been downloaded and a list of “permissions” associated with every app.
 22. As shown in the tables below, some of the findings in the survey are based on an analysis of the 960 apps while others are based on the more detailed analysis of the subset of 400 apps.
 23. Most apps are not expensive but all sales are final in the Apple App store (see iTunes Store Terms and Conditions, <http://www.apple.com/legal/itunes/us/terms.html#GIFTS> (last visited Jan. 17, 2012)) and refunds for apps obtained through the Android Market must be made within 15 minutes from download (see *Returning Apps*, Android Market Help Articles, <http://support.google.com/androidmarket/bin/answer.py?hl=en&answer=134336> (last visited Jan. 17, 2012)).
 24. See Appendix, pages A2-A3 for additional information about the differences; see also Armando Rodriguez, PC World, “Web-based Android Market Looks Good” (Feb. 2, 2011), http://www.pcworld.com/article/218532/webbased_android_market_looks_gocd.html (“Essentially it is

- the same information you would get from browsing the Market on your phone only in a much nicer-looking package.”).
25. *See* Appendix, page A3-A4 for more information about how staff categorized the apps.
 26. The “Other” category mostly included apps offering parenting guides, and children’s television or movie recommendations. Staff also encountered three apps for parents to use to monitor their child’s geolocation.
 27. *See* Appendix, page A3-A4 for additional information.
 28. In total, 5% of the 400 apps closely reviewed by staff were likely not intended to be used by kids, based on the apps’ descriptions. Except where noted, staff did not remove these apps from the analysis in this report. *See* Appendix, page A7.
 29. Staff converted the grade kindergarten to the age 5, first grade to the age 6, second grade to the age 7, etc.
 30. A recent study looking at the paid apps in the Apple App Store’s Education category found 58% of the apps were for toddlers and preschool age children. Carly Shuler, Joan Ganz Cooney Center, *iLearn II: An Analysis of the Education Category of Apple’s App Store*, 13-14 (Jan. 2012), available at <http://joanganzcooneycenter.org/Reports-33.html>.
 31. Developers do not receive compensation from the app stores when a user downloads a free app. Developers can still make money from such apps, however. As discussed below, one of the common business models is to partner with a mobile ad network that will pay a developer to include code in the app software that allows the ad network to serve ads.
 32. Several apps in the study appeared to be quite popular. One Android app appeared to have been downloaded between 5,000,000 and 10,000,000 times; six Android apps showed 1,000,000 to 5,000,000 downloads; five Android apps showed 500,000 to 1,000,000 downloads; and 19 Android apps showed that they had been downloaded 100,000 to 500,000 times.
 33. The percentages reported were calculated using the lower values of the download ranges. *See* Appendix, page A4 for more information about the download calculation.
 34. Currently, both the mobile and desktop versions of the Android Market include an email contact on the app promotion pages. At the time staff collected the information for this report, however, only the mobile version of the Android Market included this information. Therefore, the 13% figure would likely be higher if staff had captured the mobile version of the app promotion pages, or if staff were to repeat the information collection today. *See* Appendix, page A2.
 35. Staff used an English language configured browser to visit developer websites, but nevertheless encountered five foreign language websites.
 36. Because staff only reviewed the landing page of the associated websites, there may have been apps that included contact information on subsequent pages of the associated site. *See* Appendix, page A4-A5.
 37. These percentages do not add up to the 65% total because the landing pages contained different combinations of contact information.
 38. As noted, staff encountered a significant number of apps for very young children. These children are unlikely to be able to type sensitive personal information into the mobile device. Nevertheless, the app may collect and share information about the device and/or child, such as the device’s location or phone number, or other information stored on the device by the user.
 39. *See Press Release, Future of Privacy Forum, supra* note 15 (“Application developers can access a considerably broader range of information about users than traditional web developers”); Lookout Mobile Security, *App Genome Report* (Feb. 2011), available at www.mylookout.com/appgenome/ (finding that 28% of the free apps in the Android Market and 34% of the free apps in the Apple App Store have the capability to access user location information, and 7.5% of the free apps in the Android Market and 11% of the free apps in the Apple App Store have the capability to access user contacts); Thurm & Kane, *supra* note 17 (documenting the data collection that occurred through many popular smartphone apps).
 40. *See, e.g., Consumer Privacy and Protection in the Mobile Marketplace: Hearing before the Subcomm. on Consumer Protection, Product Safety and Insurance of the S. Comm. on Commerce, Science and*

Transportation. 112th Cong. 6-7 (May 10, 2011) (prepared statement of Alan Davidson, Director of Public Policy, Google Inc.), available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=517bc26f-ab89-4339-ad0f-441879598ed1 (the user may choose to trust the application by completing the installation or the user may choose to cancel the installation).

41. Android provides consumers with a very technical description of this permission stating that it allows “an application to create network sockets.” See Appendix, page A5.
42. For purposes of Table 7, staff removed any apps determined by staff not to be for kids.
43. “Phone calls: read phone state and identity” allows the app to determine if the mobile device is currently making a telephone call – presumably so that it can avoid interrupting the call. It can also determine the mobile device’s telephone number. A more descriptive list of the Android operating system permissions found in this survey is provided on pages A5-A6 of the Appendix.
44. “Modify/delete SD card” means the app would have the ability to save and erase data on the mobile device’s memory card. See Appendix, pages A5-A6.
45. See *Apple Answers the FCC’s Questions*, Apple Inc. (Aug. 21, 2009), available at <http://www.apple.com/hotnews/apple-answers-fcc-questions> (stating that it provides guidelines to developers that are used in considering whether to approve applications, and describing Apple’s review process).
46. At least one survey of free apps in the Apple App Store and the Android Market, however, found little difference between the two stores in the prevalence of access to sensitive data. Lookout Mobile Security, *supra* note 39, Figs 9-10; see also Thurm & Kane, *supra* note 17, (documenting the data collection that occurred through many popular smartphone apps).
47. *Apple Answers the FCC’s Questions*, *supra* note 45.
48. See *Consumer Privacy and Protection in the Mobile Marketplace: Hearing before the Subcomm. on Consumer Protection, Product Safety and Insurance of the S. Comm. on Commerce, Science and Transportation*, 112th Cong. 3 (May 19, 2011) (prepared statement of Catherine Novelli, Vice President, Worldwide Government Affairs, Apple Inc.), available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=4e365814-c929-4785-9d39-596052ab3a7d (stating “we make it very clear in our App Store Review Guidelines that any App that targets minors for data collection will be rejected.”).
49. See Statement of Catherine Novelli, *supra* note 48, at 4-5 (“An arrow icon alerts iOS 4 users that an application is using or has recently used location-based information”); *Understanding the LocationListener in Android*, DoityourselfAndroid.com (Dec. 25, 2010) <http://blog.doityourselfandroid.com/2010/12/25/understanding-locationlistener-android/> (discussing the GPS icon on Android and stating that “No GPS icon will be shown in the title bar, unless a certain application (like Google Maps) triggers it to request a location.”).
50. See Statement of Catherine Novelli, *supra* note 48, at 4; Statement of Alan Davidson, *supra* note 40, at 5-6.
51. See Statement of Catherine Novelli, *supra* note 48, at 4.
52. See *Best Practices for Mobile Applications Developers*, Future of Privacy Forum, 3, <http://www.futureofprivacy.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf> (last visited Jan. 24, 2012) (citing section 3.3.10 of the iOS Developer Program License Agreement, stating that “Developers must provide clear and complete information to users regarding collection, use and disclosure of user or device data.”); Android Market Developer Distribution Agreement, 4.3, <http://www.android.com/us/developer-distribution-agreement.html> (last visited Oct. 31, 2011) (“If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your Product, and you must provide legally adequate privacy notice and protection for those users.”).
53. Apple Privacy Policy, <http://www.apple.com/privacy> (last visited Jan. 17, 2012) (“Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.”); Android Privacy Policy, <http://www.android.com/privacy.html> (last visited Jan. 17, 2012) (“Information collected by the third party application provider is governed by their privacy policies.”).

54. The desktop version of the Apple App Store provides standardized locations on each app's preview page for placing links to the developer's website, a support site, and an application license agreement. Staff only reviewed the developer website link. *See* Appendix, pages A4-A5.
55. As noted in the FTC staff's preliminary privacy report, consumers are unlikely to read disclosures buried in privacy policies or "terms of service" agreements because they are not easily accessible and are invariably long, legalistic, and difficult to understand. These concerns are heightened in the mobile space, where consumers are interacting with very small screens. The privacy report encouraged companies to offer short, easy-to-read, "just in time" disclosures (or icons) that consumers are likely to see, read, and understand. *See* FTC Preliminary Staff Report, *supra* note 7, at 69-71.
56. *See* Cecilia Kang, *Lawmakers urge FTC to investigate free kids games on iPhone*, Washington Post, Feb. 8, 2011, available at <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/08/AR2011020805721.html>.
57. *See* *Administering In-app Billing*, Android Developers Guide, http://developer.android.com/guide/market/billing/billing_integrate.html (last visited Jan. 17, 2012).
58. A few applications indicated integration with more than one social network.
59. In-app advertising typically involves a relationship between the app developer and an ad network, where the ad network pays the developer to incorporate the ad network's code into the developer's application. When the app is running, the ad software allows the ad network to send ads to the user's device. Depending on how the ad network software is configured, the ad network may collect information from the user to provide targeted ads. *See* Thurm & Kane, *supra* note 17 ("[M]any ad networks offer software 'kits' that automatically insert ads into an app. The kits track where users spend time inside the app."); *see generally* *Google Ads for Mobile FAQ*, http://code.google.com/mobile/afma_ads/kb/ (last visited Jan. 17, 2012) (describing the integration of ad software for targeted advertising); iAd, <http://developer.apple.com/iad/> (last visited Jan. 17, 2012) (describing the integration of ad features in iOS).
60. *See* Jolie O'Dell, *The Rise of Mobile In-App Ads* (July 16, 2011), <http://mashable.com/2011/07/16/in-app-ads/> (43% of the app developers used in-app advertising in 2011).
61. Other organizations review mobile apps and provide ratings and recommendations to help parents select content appropriate apps for kids. *See, e.g.*, Common Sense Media, *Best apps: Our recommendations for families*, <http://www.commonsensemedia.org/mobile-app-lists> (last visited Jan. 17, 2012).
62. While reviewing the app promotion pages in the survey, staff did not encounter any references to the age and content ratings found on many computer and video games, which are assigned by the Entertainment Software Rating Board (ESRB). Staff also notes that the ESRB and the wireless trade association CTIA have recently created a new mobile app rating system that uses its traditional icons to inform users. *See* Press Release, ESRB, *CTIA-The Wireless Association and ESRB Announce Mobile Application Rating System* (Nov. 29, 2011), available at http://www.esrb.org/about/news/downloads/CTIA_ESRB_Release_11.29.11.pdf. Like the Apple and Android rating systems, this new ratings system considers whether the app contains violence, language, or sexual content. It also considers whether the app has a minimum age requirement, allows the exchange of user-generated content, or enables users to share their location with other app users. However, this system also relies on developer provided information. Apple and Google are not currently participating in this initiative. *See* Kevin Fitchard, *Apple, Google Absent From ESRB's New Mobile App Rating System*, Gigaom (Nov. 29, 2011), <http://gigaom.com/2011/11/29/apple-google-absent-from-esrbs-new-mobile-app-rating-system/>.
63. *See, e.g.*, Statement of Catherine Novelli, *supra* note 48, at 2; *iTunes: Using Parental Controls*, Apple, <http://support.apple.com/kb/ht1904> (last modified Sept. 23, 2011). The Android Market allows users to filter apps displayed in the market based on app content ratings. *Application Content Ratings*, Android Market, <http://support.google.com/androidmarket/bin/answer.py?hl=en&answer=1075738> (last visited Jan. 17, 2012).
64. *See* Apple, *iTunes Connect Developer Guide, Version 7.2* 52-53 (Oct. 17, 2011), available at https://itunesconnect.apple.com/docs/iTunesConnect_DeveloperGuide.pdf; Statement of Alan Davidson, *supra* note 40, at 7.

65. See *iTunes Connect Developer Guide*, *supra* note 64, at 52.
66. *Id.*
67. *Rating Your Application Content for Android Market*, Android Market for Developer, <http://support.google.com/androidmarket/developer/bin/answer.py?hl=en&answer=188189> (last visited Jan. 17, 2012).
68. *Id.*
69. *Id.*
70. Staff did not evaluate the appropriateness of the Android ratings, but noticed that four of the Android “kids” apps listed a “medium maturity” rating, and four others listed a “high maturity” rating. Upon further review of these app descriptions, only five of these eight apps appeared to be intended for a child to use. These five apps consisted of three flashcard games, one painting game, and one “animal sounds” game. Based on the information available, staff could not determine why these five apps had such high maturity ratings.
71. See Apple, *iOS: Understanding Restrictions*, available at <http://support.apple.com/kb/ht4213> (last modified Oct. 24, 2011); Kids and Media, *Parental Controls for Android* (Dec. 5, 2011), www.kidsandmedia.org/parent-controls-for-android/; see also *Application Content Ratings*, Android Market, *supra* note 63.
72. See Apple, *iOS: Understanding Restrictions*, *supra* note 71.
73. See Kids and Media, *Parental controls for Android*, *supra* note 71; iKid Apps, *How to Setup Parental Controls on Android* (July 22, 2011) available at <http://www.ikidapps.com/2011/07/how-to-setup-parental-controls-on-android.html>.
74. For example, a child may not be able to access higher levels of a game or additional content if the internet connection has been blocked.

Appendix

Methodology

This section provides additional information about the data collected and reviewed in the attached FTC Staff Report on Kids Apps.

Apple Data Collection

On July 14, 2011, staff used a desktop computer with the Windows 7 operating system to locate and copy the app store promotion pages for 960 mobile applications using the following steps. Staff first searched on the term “kids” in the desktop version of Apple’s iTunes app store and noted that each app had its own nine-digit unique identifier number and its own app store promotion page describing the app. The app store promotion page for each app was viewable by typing in the specific web address within the itunes.apple.com website, which contained the unique app identifier number, into the Internet Explorer browser on the desktop computer. Thus, staff could locate the unique web address for each app store promotion page using the following convention “http://itunes.apple.com/us/app/id[9-digit-unique-app-identification-number]?mt=8.” Staff then used software to visit and copy the browser-viewable app promotion pages for the first 480 apps returned by the “kids” search in the Apple app store.

Android Data Collection

On July 14, 2011, staff used the same desktop computer with the Internet Explorer browser to access the desktop version of the Android Market, available at <https://market.android.com>. Staff searched on the term “kids” and noted that each app had its own unique identifier and its own app store promotion page describing the app. Like Apple, the Android Market app promotion page for each app was viewable by typing in the specific web address within the market.android.com website, which contained the unique app identifier, into the browser. Staff could locate the unique web address for each app store promotion page using the following convention, “https://market.android.com/details?id=[unique-app-id]&feature=search_result.” Staff then used software to visit and copy the app promotion pages for the first 480 Android Market apps returned by the “kids” search.

Data Extraction

Staff saved each app store promotion page as a .txt file and as an .html file. Staff identified the relevant fields, such as price, developer, and number of ratings, found within the

copied app promotion pages and extracted that data into an electronic database. This automated extraction was the source of all of the n=480 tables in the report.

Reviewing the Random Sample of App Store Promotion Pages

Staff completed a review of 400 randomly selected app store promotion pages. For each of the pools of the 480 app promotion pages, staff used a random number generator to select 200 unique numbers and created a separate database that contained only the 200 app store promotion pages that corresponded with the 200 randomly selected numbers. Reviewers were instructed to examine the electronically captured app promotion pages (that had been saved as .html files), and to answer a series of questions about things like app topic, age range, and disclosures related to their review of the app promotion page using the database form. The specific instructions related to this review are detailed below. Once staff completed the review, two additional reviewers rated the sample, and found almost complete agreement between the first and second review, suggesting that the application of staff's criteria was relatively unambiguous.

Reviewers were also instructed to click on the website address listed on the app promotion page in the field for “[developer’s] website.” Staff then saved and reviewed the resulting webpage (the “landing page” of the developer’s website), and entered the answers to a series of questions using the database form. Tables containing calculations that list “n=200” specify that the calculations were obtained from one of the two random samples.¹

App Store Desktop Interface v. Mobile Device Interface

Staff collected the information in this report only from the content offered in the desktop interface of the two app stores. There are two relevant differences between this content and the content available through the mobile device interface, but staff does not believe these differences change the conclusions of this report.

App store promotion pages viewed in the Android Market using a mobile device include a field that displays a developer email address. At the time staff collected the information for the survey, this field was not found on the desktop version of the Android Market, and, thus, was not captured in the survey. Therefore, more email addresses were likely available for the Android apps in this survey than staff collected.

1. The specific random sample used is identified by the column heading under which the “n=200” specification is found.

Similarly, app store promotion pages viewed in the desktop version of Apple’s App Store included a field that displayed a web address labeled “[Developer Name] Support,” even though this field was not found in promotion pages viewed from an iPhone. As noted in the report, staff did not review these additional web addresses and does not know if they contained additional contact information or disclosure information. Staff did note that 61% of the promotion pages listed the same address for both the developer’s website and the support website.

Categorizing Apps based on Type

Staff categorized the apps in the random sample based on a number of categories according to words found within the app descriptions and titles. The following is a list of the categories and any additional words used to classify an app into the categories: Educational (“learn,” “teach,” or any variation of the word “educate”); Game (“play”); Animal-related (“animal,” “creatures,” or the names or icons of different types of animals); Alphabet/Spelling/Words (“letters”); Math/Numbers (“arithmetic,” “counting,” “addition,” “subtraction,” “multiplication,” or “division”); Matching (“match,” or “find 2 of the same”); Memory; Book/Story (“chapters”); Coloring (“paint” or “draw”); Musical (“music” or “song”); Puzzle; Learning a language²; Flash Cards; Photo-related (“photo” or “picture”); Quiz/Test; Jokes; and other. Apps could fall into more than one category. For example, a matching game that involved pictures of animals would be categorized under “Game,” “Matching,” and “Animal-related.”

Categorizing Apps based on Intended User

Staff categorized the 400 apps in the random sample based on whether the app title or description identified any one of the following groups as an audience for whom the app was intended or recommended: Infant; Toddler; Child; Kid; Teen; Adult; Parent; Teacher; Family; Mature; Everyone; Preschool; Elementary; Middle School; High School; Age Range; Grade Range; Other; and No Indication. Grade and age range information have been presented separately from the qualitative categories in the report. Simply containing one of these audience groups in the app title or description was not sufficient to trigger an intended use category. The app title or description had to indicate in some way that the app was for one or more of these groups’ use. For example, one of the promotion pages described an app containing recipes for child-friendly meals. Although the description included the term “child,”

2. This category only included apps that had the word “learn” plus a language in the title or description.

the app was intended for use by parents or caretakers to make meals for children and therefore was not included in the “child” category.

Price Level Popularity

To estimate price level popularity for the Android apps in the survey, staff summed the lower bound of the download range for each app within a given price level. Next, staff divided these price level sums by the sum of the lower bound of the download ranges for all 480 Android apps. Using this method, staff found that the free Android apps returned by the “kids” search, which accounted for 62% of the search results, accounted for 99% of all downloads. Table 7 of the report contains the results obtained using the lower bound method.

Staff then repeated its calculations using the upper bound and midpoint of each download range. Staff found that the results returned by each method were nearly indistinguishable from the results obtained using the lower bound of the download ranges.

Both the Android Market and the Apple App Store display the number of users that have provided feedback for a particular app. Staff used this feature to estimate price level popularity for the Apple apps, and as a second estimate of app popularity for the Android apps, by repeating the calculations described above substituting the number of feedbacks for downloads.

Developer Websites

Both the Apple App Store and the Android Market provide a specified field on the app store promotion page for developers to list their website. Although some app store promotion pages additionally listed web addresses in other places (such as the text of the app description), staff restricted its review to the landing page of the developer website address listed in the developer web address field. Staff found that a sizeable number of the website addresses listed in the developer web address field did not lead to relevant or functioning websites.

Of the 400 randomly selected “kids” app promotion pages reviewed by staff, 43 (11%) did not list a web address in the specified field for developer website; 17 (4%) listed a web address that staff was unable to examine; and 10 (3%) listed a web address that either led back to the app promotion page, or was not related to the app or developer in any apparent way. Staff was unable to examine websites when they encountered problems including: error messages (such as “site not found” or “site under construction” messages); never-ending redirects; “access forbidden” messages; and one Facebook page that required the visitor to be logged into Facebook in order to access the webpage. In addition, 5 (1%) of the web addresses led to websites that were entirely in a foreign language (even though staff used an English

language browser and browsed US app stores), and therefore were not counted. In the end, 324 (81%) of the 400 “kids” app promotion pages listed a web address in the specified field that led to a functioning and relevant English language webpage.

Web Addresses in the Standardized Locations in the Apple App Store

The Apple App Store desktop version provides developers with standardized locations on each app’s promotion page for placing links to the developer’s website, a support site, and an application license agreement. Most Apple app store promotion pages in the survey contained a link to a developer website (469 out of 480, or 97.7%), and all of the pages contained a link to a support website. A few contained a link to an application license agreement (6 out of 480, or 1.3%). As stated above, 61% of the promotion pages listed the same address for both the developer’s website and the support website. Staff did not look at the remaining 39%; it is possible that more of the pages linked to additional privacy disclosures or developer contact information.

Other Websites

Reviewers also noted any web addresses listed on the app promotion pages outside of the app store standardized locations. While a number of developers used their app description space on the page to encourage readers to like them on Facebook, or follow them on Twitter, only 8% of the 400 app promotion pages reviewed by staff provided an address to an additional website.

Android Permissions Language

Below is a list of the Android disclosures identified in Table 7 of the report, taken verbatim from the app promotion pages encountered in this survey. While each disclosure is reported in its entirety, the list is not exhaustive of those used in the Android Market or found in the samples associated with this report.

- “Network communication > full Internet access > Allows an application to create network sockets.”
- “Phone calls > read phone state and identity > Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.”
- “Modify/delete SD card contents > Allows an application to write to the USB storage. Allows an application to write to the SD card.”

- “Your location > coarse (network-based) location > Access coarse location sources such as the cellular network database to determine an approximate device location, where available. Malicious applications can use this to determine approximately where you are.”
- “Your location > fine (GPS) location > Access fine location sources such as the Global Positioning System on the device, where available. Malicious applications can use this to determine where you are, and may consume additional battery power.”
- “Hardware controls > take pictures and videos > Allows application to take pictures and videos with the camera. This allows the application at any time to collect images the camera is seeing.”
- “Services that cost you money > directly call phone numbers > Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.”
- “System tools > modify global system settings > Allows an application to modify the system’s settings data. Malicious applications can corrupt your system’s configuration.”
- “Hardware controls > record audio > Allows application to access the audio record path.”
- “Your personal information > read sensitive log data > Allows an application to read from the system’s various log files. This allows it to discover general information about what you are doing with the device, potentially including personal or private information.”

Implications of Methodology and Interpretation of Results

Survey designs inevitably make tradeoffs; presenting evidence in ways that shed the most light on some questions necessarily leave other issues unaddressed. Searching the app stores using the word “kids” is a transparent methodology that works in both app stores and generates a diverse and relevant set of results; however, it is important to bear in mind the following implications of the survey design:

The first 480 apps returned by each query³ were given both equal importance and equal likelihood of inclusion in the random sample. This means that the report’s findings relate to overall performance from the field of apps for kids, rather than giving extra weight to those with more downloads.

3. Searches on the Android Market only yield 480 accessible results. Staff considered all 480 Android Market results, and truncated the results from the Apple App Store to 480 in order to make the samples comparable.

Staff did not remove the small handful of apps from the random sample that may not be intended for kids. However, these non-kid apps are rare enough that excluding them would not significantly change the report's findings.

The algorithms responsible for returning search results differ between the Android Market and the Apple App Store, which likely rely on keywords and other information to render search results.⁴ Staff is not privy to the precise formulas, and using other search terms or selecting apps in different ways might generate somewhat different results.

These issues suggest exercising caution in claiming that the percentages found in the report extend to samples of apps beyond that used by this report. However, none of these issues change the conclusion that kids' app promotion pages that make few disclosures are widespread and easy to find.

4. For this reason, it is not surprising that only 61.5% of the Apple app promotion pages and 72.5% of the Android app promotion pages indicated they were intended to be used by "kids."

1 TONY WEST
Assistant Attorney General
2 Civil Division
U.S. Department of Justice
3

4 KENNETH L. JOST
Acting Director
Office of Consumer Protection Litigation
5

6 ALAN PHELPS
Trial Attorney
Office of Consumer Protection Litigation
7 U.S. Department of Justice
P.O. Box 386
8 Washington, DC 20044
Telephone: 202-307-6154
9 Fax: 202-514-8742
10 Email: alan.phelps@usdoj.gov

11 Attorneys for the Plaintiff

12 UNITED STATES DISTRICT COURT
13 NORTHERN DISTRICT OF CALIFORNIA
San Jose Division

14 UNITED STATES OF AMERICA,
15 Plaintiff,

16 v.

17
18 W3 INNOVATIONS, LLC,
a limited liability company,
19 also doing business as
Broken Thumbs Apps, and

20 JUSTIN MAPLES,
21 individually an as an officer of
W3 INNOVATIONS, LLC,
22 Defendants.

CV 11-03958

PSG

CONSENT DECREE AND ORDER
FOR CIVIL PENALTIES, INJUNCTION,
AND OTHER RELIEF

23 WHEREAS Plaintiff, the United States of America, has commenced this action by filing
24 the complaint herein; Defendants have waived service of the Summons and Complaint; the
25 parties have been represented by the attorneys whose names appear hereafter; and the parties
26 have agreed to settlement of this action upon the following terms and conditions, without
27 adjudication of any issue of fact or law, and without Defendants admitting that any issue of fact
28 or law other than those relating to jurisdiction and venue is true;

1 THEREFORE, on the joint motion of Plaintiff and Defendants, it is hereby ORDERED,
2 ADJUDGED, and DECREED as follows:

3 1. This Court has jurisdiction of the subject matter and of the parties pursuant to 28 U.S.C.
4 §§ 1331, 1337(a), 1345, and 1355, and 15 U.S.C. §§ 45(m)(1)(A), 53(b), 56(a), and 57b.

5 2. Venue is proper as to all parties in the Northern District of California under 15 U.S.C.
6 § 53(b) and 28 U.S.C. §§ 1391(b)-(c) and 1395(a).

7 3. The activities of Defendants are in or affecting commerce as defined in Section 4 of the
8 FTC Act, 15 U.S.C. § 44.

9 4. The Complaint states a claim upon which relief may be granted against Defendants under
10 Sections 1303(c) and 1306(d) of the Children's Online Privacy Protection Act of 1998
11 ("COPPA"), 15 U.S.C. §§ 6501-6506, 6502(c), and 6505(d); the Commission's
12 Children's Online Privacy Protection Rule, 16 C.F.R. Part 312; and Sections 5(a)(1),
13 5(m)(1)(A), 13(b), and 16(a) of the Federal Trade Commission Act ("FTC Act"), 15
14 U.S.C. §§ 41-58, 45(a)(1), 45(m)(1)(A), 53(b), and 56(a). Among other things, the
15 complaint alleges that Defendants violated COPPA by failing to provide notice to parents
16 of their information practices, and by failing to obtain verifiable parental consent prior to
17 collecting, using, and/or disclosing personal information from children online.

18 5. Defendants have entered into this Consent Decree and Order for Civil Penalties,
19 Injunction, and Other Relief ("Order") freely and without coercion. Defendants further
20 acknowledge that they have read the provisions of this Order and are prepared to abide
21 by them.

22 6. Plaintiff and Defendants hereby waive all rights to appeal or otherwise challenge the
23 validity of this Order.

24 7. Plaintiff and Defendants stipulate and agree that entry of this Order shall constitute a full,
25 complete, and final settlement of this action.

26 8. Defendants have agreed that this Order does not entitle them to seek or to obtain
27 attorneys' fees as a prevailing party under the Equal Access to Justice Act, 28 U.S.C.
28 § 2412, and Defendants further waive any rights to attorneys' fees that may arise under

1 said provision of law.

2 9. Entry of this Order is in the public interest.

3 **DEFINITIONS**

4 10. "Rule" means the Federal Trade Commission's Children's Online Privacy Protection
5 Rule, 16 C.F.R. Part 312.

6 11. The terms "child," "collects," "collection," "Commission," "delete," "disclosure,"
7 "Internet," "online contact information," "operator," "parent," "person," "personal
8 information," "third party," "verifiable consent," and "website or online service directed
9 to children," mean as those terms are defined in Section 312.2 of the Rule, 16 C.F.R.
10 § 312.2.

11 12. "Individual Defendant" means Justin Maples.

12 13. "Corporate Defendant" means W3 Innovations, LLC, and its successors and assigns.

13 14. "Defendants" means the Individual Defendant and the Corporate Defendant, individually,
14 collectively, or in any combination.

15 **INJUNCTION**

16 15. **IT IS ORDERED** that Defendants, and their officers, agents, representatives, and
17 employees, and all persons in active concert or participation with them who receive
18 actual notice of this Order by personal service or otherwise, are hereby enjoined, directly
19 or through any corporation, subsidiary, division, website, or other device, from:

20 A. Failing to provide sufficient notice of what information Defendants collect online
21 from children, how they use such information, their disclosure practices, and all
22 other content, on any website or online service that is directed to children, or any
23 website or online service through which they, with actual knowledge, collect, use,
24 and/or disclose personal information from children, as required by Section
25 312.4(b) of the Rule, 16 C.F.R. § 312.4(b);

26 B. Failing to provide direct notice to parents of what information Defendants collect
27 online from children, how they use such information, their disclosure practices,
28 and all other required content, in connection with any website or online service

1 that is directed to children, or any website or online service through which they,
2 with actual knowledge, collect, use, and/or disclose personal information from
3 children, as required by Section 312.4(c) of the Rule, 16 C.F.R. § 312.4(c);

4 C. Failing to obtain verifiable parental consent before any collection, use, and/or
5 disclosure of personal information from children, in connection with any website
6 or online service that is directed to children, or on any website or online service
7 through which they, with actual knowledge, collect, use, and/or disclose personal
8 information from children, as required by Section 312.5 of the Rule, 16 C.F.R. §
9 312.5(a)(1); or,

10 D. Violating any other provision of the Children's Online Privacy Protection Rule,
11 16 C.F.R. Part 312, and as the Rule may hereafter be amended. A copy of the
12 Rule is attached hereto as "Appendix A" and incorporated herein as if fully set
13 forth verbatim.

14 **DELETION OF CHILDREN'S PERSONAL INFORMATION**

15 16. **IT IS FURTHER ORDERED** that Defendants, within five (5) days from the date of
16 entry of this Order, shall delete all personal information collected and maintained in
17 violation of the Rule at any time from April 21, 2000 through the date of entry of this
18 Order.

19 **CIVIL PENALTY**

20 17. **IT IS FURTHER ORDERED** that Defendants, jointly and severally, shall pay to
21 Plaintiff a civil penalty, pursuant to Section 5(m)(1)(A) of the FTC Act, 15 U.S.C.
22 § 45(m)(1)(A), in the amount of fifty thousand dollars (\$50,000).

23 18. Prior to or concurrently with Defendants' execution of this Order, Defendants shall turn
24 over the full amount of the civil penalty to their attorneys, who shall hold the entire sum
25 for no purpose other than payment to the Treasurer of the United States after entry of this
26 Order by the Court. Within five (5) days of receipt of notice of the entry of this Order,
27 Defendants' attorneys shall transfer the sum of \$50,000 in the form of a wire transfer or
28 certified cashier's check made payable to the Treasurer of the United States. The check

1 and/or written confirmation of the wire transfer shall be delivered in accordance with
2 procedures specified by the Office of Consumer Litigation, Civil Division, U.S.
3 Department of Justice, Washington, DC 20530.

4 19. Defendants relinquish all dominion, control, and title to the funds paid to the fullest
5 extent permitted by law. Defendants shall make no claim to or demand return of the
6 funds, directly or indirectly, through counsel or otherwise.

7 20. Defendants agree that the facts as alleged in the Complaint filed in this action shall be
8 taken as true, without further proof, in any subsequent civil litigation filed by or on
9 behalf of the Commission solely to enforce its rights to any payment or money judgment
10 pursuant to this Order.

11 21. Defendants agree that the judgment represents a civil penalty owed to the United States
12 Government, is not compensation for actual pecuniary loss, and, therefore, as to the
13 Individual Defendant, is not subject to discharge under the Bankruptcy Code pursuant to
14 11 U.S.C. § 523(a)(7).

15 22. In the event of any default in payment, which default continues for ten (10) days beyond
16 the due date of payment, the entire unpaid penalty, together with interest, as computed
17 pursuant to 28 U.S.C. § 1961 (accrued from the date of default to the date of payment)
18 shall immediately become due and payable.

19 **COMPLIANCE MONITORING**

20 23. **IT IS FURTHER ORDERED** that for the purpose of monitoring and investigating
21 compliance with any provision of this Order:

22 A. Within ten (10) days of receipt of written notice from a representative of the
23 Commission, Defendants each shall submit written reports, which are true and
24 accurate and sworn to under penalty of perjury; produce documents for inspection
25 and copying; appear for deposition; and provide entry during normal business
26 hours to any business location in each Defendant's possession or direct or indirect
27 control to inspect the business operation. Provided that Defendants, after
28 attempting to resolve any dispute without court action and for good cause shown,

1 may file a motion with this Court seeking an order including one or more of the
2 protections set forth in Fed. R. Civ. P. 26(c).

3 B. In addition, the Commission is authorized to use all other lawful means, including
4 but not limited to:

- 5 1. Obtaining discovery from any person, without further leave of court, using
6 the procedures prescribed by Fed. R. Civ. P. 30, 31, 33, 34, 36, 45 and 69;
- 7 2. Having its representatives pose as consumers and suppliers to Defendants,
8 their employees, or any other entity managed or controlled in whole or in
9 part by any Defendant, without the necessity of identification or prior
10 notice; and,

11 C. Defendants each shall permit representatives of the Commission to interview any
12 employer, consultant, independent contractor, representative, agent, or employee
13 who has agreed to such an interview, relating in any way to any conduct subject
14 to this Order. The person interviewed may have counsel present, including
15 Defendants' counsel and any individual counsel.

16 D. For purposes of the compliance reporting and monitoring required by this Order,
17 the Commission is authorized to communicate directly with each Defendant.

18 *Provided however*, that nothing in this Order shall limit the Commission's lawful use of
19 compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49,
20 57b-1, to obtain any documentary material, tangible things, testimony, or information
21 relevant to unfair or deceptive acts or practices in or affecting commerce (within the
22 meaning of 15 U.S.C. § 45(a)(1)).

23 **COMPLIANCE REPORTING**

24 24. **IT IS FURTHER ORDERED** that, in order that compliance with the provisions of this
25 Order may be monitored:

26 A. For a period of three (3) years from the date of entry of this Order,

27 1. Individual Defendant shall notify the Commission of the following:

28 a. Any changes in such Defendant's residence, mailing address, and

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

telephone number, within ten (10) days of the date of such change;

b. Any changes in such Defendant's employment status (including self-employment), and any change in such Defendant's ownership in any business entity, within ten (10) days of the date of such change. Such notice shall include the name and address of each business that such Defendant is affiliated with, employed by, creates or forms, or performs services for; a detailed description of the nature of the business; and a detailed description of such Defendant's duties and responsibilities in connection with the business or employment; and,

c. Any changes in such Defendant's name or use of any aliases or fictitious names within ten (10) days of the date of such change;

2. Defendants shall notify the Commission of any changes in structure of the Corporate Defendant or any business entity that any Defendant directly or indirectly controls, or has an ownership interest in, that may affect compliance obligations arising under this Order, including but not limited to: incorporation or other organization; a dissolution, assignment, sale, merger, or other action; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; or a change in the business name or address, at least thirty (30) days prior to such change, *provided that*, with respect to any such change in the business entity about which a Defendant learns less than thirty (30) days prior to the date such action is to take place, such Defendant shall notify the Commission as soon as is practicable after obtaining such knowledge.

B. Sixty (60) days after the date of entry of this Order, and thereafter for a period of three (3) years, at such times as the Federal Trade Commission shall reasonably require, Defendants each shall provide a written report to the Commission, which is true and accurate and sworn to under penalty of perjury, setting forth in detail

1 the manner and form in which each has complied and is complying with this
2 Order. This report shall include, but not be limited to:

3 1. For the Individual Defendant:

- 4 a. such Defendant's then-current residence address, mailing
5 addresses, and telephone numbers;
- 6 b. such Defendant's then-current employment status (including self-
7 employment), including the name, addresses, and telephone
8 numbers of each business that such Defendant is affiliated with,
9 employed by, or performs services for; a detailed description of the
10 nature of the business; and a detailed description of such
11 Defendant's duties and responsibilities in connection with the
12 business or employment; and,
- 13 c. Any other changes required to be reported under Subsection A of
14 this Section.

15 2. For the Corporate Defendant and Individual Defendant, for any business
16 which they, individually or collectively, own a majority interest in or
17 directly or indirectly control:

- 18 a. A statement setting forth in detail the criteria and process through
19 which any of Defendant's websites or online services enable the
20 collection or disclosure of personal information, and a copy of
21 each different version of screen or page where personal
22 information can be collected or disclosed;
- 23 b. A copy of each different version of privacy notice posted on any of
24 Defendant's websites or online services;
- 25 c. A statement setting forth in detail each place where a privacy
26 notice or a link to a privacy notice is located on any website or
27 online service, and a copy of each different version of screens or
28 pages containing a privacy notice or a link to a privacy notice;

- 1 d. A copy of each different version of privacy notice sent to parents;
- 2 e. A statement setting forth in detail when and how each notice to
- 3 parents is provided;
- 4 f. A statement setting forth in detail the methods used to obtain
- 5 verifiable parental consent prior to any collection, use, and/or
- 6 disclosure of personal information from children;
- 7 g. A statement setting forth in detail the means provided for parents
- 8 to review the personal information collected from their children
- 9 and to refuse to permit its further use or maintenance;
- 10 h. A statement setting forth in detail why each type of information
- 11 collected from a child is reasonably necessary for the provision of
- 12 the particular related activity;
- 13 i. A statement setting forth in detail the procedures used to protect
- 14 the confidentiality, security, and integrity of personal information
- 15 collected from children;
- 16 j. A copy of each acknowledgment of receipt of this Order, obtained
- 17 pursuant to the Section titled "Distribution of Order"; and,
- 18 k. Any other changes required to be reported under Subsection A of
- 19 this Section.

20 C. Each Defendant shall notify the Commission of the filing of a bankruptcy petition
21 by such Defendant within fifteen (15) days of filing.

22 D. For the purposes of this Order, Defendants shall, unless otherwise directed by the
23 Commission's authorized representatives, send by overnight courier (not the U.S.
24 Postal Service) all reports and notifications to the Commission that are required
25 by this Order to the following address:
26
27
28

1 Associate Director for Enforcement
2 Bureau of Consumer Protection
3 Federal Trade Commission
4 600 Pennsylvania Avenue, NW
5 Washington, D.C. 20580
6 RE: U.S. v. W3 Innovations, LLC

7 *Provided* that, in lieu of overnight courier, Defendants may send such reports or
8 notifications by first-class mail, but only if Defendants contemporaneously send
9 an electronic version of such report or notification to the Commission at:
10 DEBrief@ftc.gov.

11 RECORD-KEEPING PROVISIONS

12 25. **IT IS FURTHER ORDERED** that, for a period of six (6) years from the date of entry of
13 this Order, Corporate Defendant and Individual Defendant, for any business engaged in
14 activities relating to the subject matter of this Order, and which they, individually or
15 collectively, own a majority interest in or directly or indirectly control, are hereby
16 restrained and enjoined from failing to create and retain the following records:

- 17 A. A print or electronic copy of all documents necessary to demonstrate full
18 compliance with each provision of this Order, including, but not limited to:
- 19 1. Copies of acknowledgments of receipt of this Order required by Sections
20 titled "Distribution of Order" and "Acknowledgment of Receipt of
21 Order";
 - 22 2. All reports submitted to the Commission pursuant to the Section titled
23 "Compliance Reporting";
 - 24 3. A sample copy of every materially different form, page, or screen through
25 which personal information is collected or disclosed, and a sample copy of
26 each materially different document containing any representation
27 regarding Defendants' collection, use, and disclosure practices pertaining
28 to personal information of a child. Each web page copy shall be
accompanied by the URL of the web page where the material was posted

1 online. Electronic copies shall include all text and graphics files, audio
2 scripts, and other computer files used in presenting information.

3 *Provided*, however, that Defendants shall not be required to retain any
4 document for longer than two (2) years after the document was created, or
5 to retain a print or electronic copy of any amended form, page, or screen
6 to the extent that the amendment does not affect Defendants' compliance
7 obligations under this Order.

8 DISTRIBUTION OF ORDER

9 26. **IT IS FURTHER ORDERED** that, for a period of three (3) years from the date of entry
10 of this Order, Defendants shall deliver copies of the Order, including Appendix A, as
11 directed below:

- 12 A. Corporate Defendant: The Corporate Defendant must deliver a copy of this Order
13 to: (1) all of its principals, officers, directors, and managers; (2) all of its
14 employees, agents, and representatives who have responsibilities related to the
15 operation of any website or online service subject to this Order; and (3) any
16 business entity resulting from any change in structure set forth in Subsection A.2.
17 of the Section titled "Compliance Reporting." For current personnel, delivery
18 shall be within five (5) days of service of this Order upon each such Defendant.
19 For new personnel, delivery shall occur prior to their assuming their
20 responsibilities. For any business entity resulting from any change in structure set
21 forth in Subsection A.2. of the Section titled "Compliance Reporting," delivery
22 shall be at least ten (10) days prior to the change in structure.
- 23 B. Individual Defendant as control person: For any business engaged in activities
24 related to the subject matter of this Order, and that the Individual Defendant owns
25 a majority interest in or directly or indirectly controls, Individual Defendant must
26 deliver a copy of this Order to: (1) all principals, officers, directors, and managers
27 of that business; (2) all employees, agents, and representatives of that business
28 who engage in activities related to the subject matter of the Order; and (3) any

1 business entity resulting from any change in structure set forth in Subsection A.2.
2 of the Section titled "Compliance Reporting." For current personnel, delivery
3 shall be within five (5) days of service of this Order upon such Defendant. For
4 new personnel, delivery shall occur prior to their assuming their responsibilities.
5 For any business entity resulting from any change in structure set forth in
6 Subsection A.2. of the Section titled "Compliance Reporting," delivery shall be at
7 least ten (10) days prior to the change in structure.

8 C. Defendants must secure a signed and dated statement acknowledging receipt of
9 the Order, within thirty (30) days of delivery, from all persons receiving a copy of
10 the Order pursuant to this Section. Defendants shall maintain copies of the signed
11 statements, as well as other information regarding the fact and manner of its
12 compliance, including the name and title of each person to whom a copy of the
13 Order has been provided and, upon request, shall make the statements and other
14 information available to the Commission.

15 **ACKNOWLEDGMENT OF RECEIPT OF ORDER**

16 27. **IT IS FURTHER ORDERED** that each Defendant, within five (5) business days of
17 receipt of this Order as entered by the Court, must submit to the Commission a truthful
18 sworn statement acknowledging receipt of this Order.

19 **PROVISION OF TAXPAYER IDENTIFYING NUMBERS**

20 28. **IT IS FURTHER ORDERED** that the Corporate Defendant is hereby required, in
21 accordance with 31 U.S.C. § 7701, to furnish to the Federal Trade Commission its
22 taxpayer identifying number (employer identification number), which shall be used for
23 purposes of collecting and reporting any delinquent amount arising out of its relationship
24 with the government.

25 **RETENTION OF JURISDICTION**

26 29. This Court shall retain jurisdiction of this matter for the purposes of construction,
27 modification, and enforcement of this Order.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JUDGMENT IS THEREFORE ENTERED in favor of Plaintiff and against
Defendants, pursuant to all the terms and conditions recited above.

Dated this 8th day of September, 2011.

Paul S. Aene
UNITED STATES XXXXXX JUDGE
Magistrate


1 The parties, by their counsel, hereby consent to the terms and conditions of the Order as
2 set forth above and consent to the entry thereof.

3 FOR THE UNITED STATES OF AMERICA:

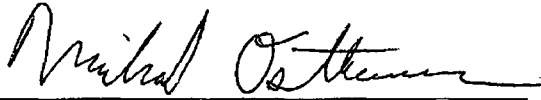
4 TONY WEST
5 Assistant Attorney General
6 Civil Division
7 U.S. Department of Justice

8 MAAME EWUSI-MENSAH FRIMPONG
9 Acting Deputy Assistant Attorney General
10 Civil Division

11 KENNETH L. JOST
12 Acting Director
13 Office of Consumer Protection Litigation

14 
15 ALAN PHELPS
16 Trial Attorney
17 Office of Consumer Protection Litigation
18 U.S. Department of Justice
19 P.O. Box 386
20 Washington, DC 20044
21 Telephone: 202-307-6154
22 Fax: 202-514-8742
23 Email: alan.phelps@usdoj.gov
24
25
26
27
28

FOR THE FEDERAL TRADE COMMISSION:



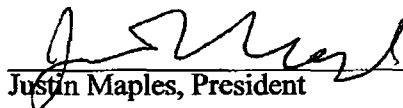
Michael Ostheimer
Attorney
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
(202) 326-2699 (voice)
(202) 326-3259 (fax)



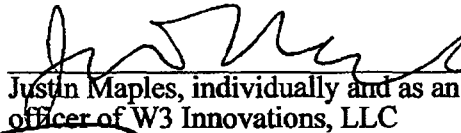
Mamie Kresses
Attorney
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
(202) 326-2070 (voice)
(202) 326-3259 (fax)

FOR THE DEFENDANTS:

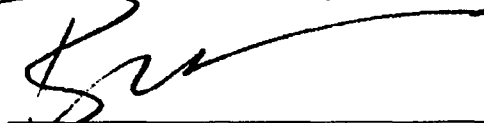
W3 INNOVATIONS, LLC



Justin Maples, President

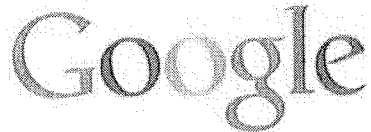


Justin Maples, individually and as an
officer of W3 Innovations, LLC



Barry J. Reingold
Perkins Coie LLP
Attorney for Defendants

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27



July 8, 2011

Ex Parte via Electronic Filing

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Public Forum on Location-Based Services*, WT Dkt No. 11-84

Dear Ms. Dortch:

We would like to thank the Wireless Telecommunications Bureau for including Google in its forum on location-based services. Google shares the Commission's excitement about the value these services will bring to Americans and its commitment to transparency, user control, and security in the collection and use of location data.

Over the last two years, location-based services have shifted from the purview of early adopters to a fact of life for millions. People can use mobile services to get driving directions from their current location, identify a traffic jam and find an alternate route, or find an open pharmacy at 2 AM for a sick child. In the last year, a full 40% of Google Maps usage was from mobile devices. There are now 150 million active monthly Google Maps for Mobile users on Android, iPhone, BlackBerry, and other mobile platforms in more than 100 countries.

Mobile location data can even save lives. Emergency notifications like AMBER Alerts can be improved using location data — within seconds of the first report, an AMBER Alert could be distributed to all users within one mile of the incident. This is just one example of the benefits these services can provide. A recent study by McKinsey estimates that personal location applications will generate as much as \$700 billion in consumer value in the next eight years.

Google would not be able to offer these services — or help create the economic and social value generated from location data — if we lost the trust of our users. We understand location information is sensitive, so our approach to location data is simple: Opt-in consent and clear notice are required for collection and use of location information on Android. We don't collect any location information — any at all — through our location services on Android devices unless the user specifically chooses to share this information with Google. We also give users clear notice and control; the set-up process explicitly asks users to "allow Google's location service to collect

Ex Parte Filing, WT Dkt No. 11-84

July 8, 2011

Page 2

anonymous location data.” And even after the set-up process, users can easily turn off location sharing with Google at any time they wish. We hope that this will be a standard for the industry.

To learn more about Google’s approach to location-based services and user privacy, please see our recent testimony before the Senate Commerce Committee, which is attached to this letter.

Pursuant to the Commission’s rules, this notice is being filed in the above referenced docket for inclusion in the public record.

Sincerely,

A handwritten signature in black ink, appearing to read "Alan B. Davidson", with a long horizontal flourish extending to the right.

Alan B. Davidson
Director, Public Policy
Google Inc.

Attachment



Testimony of Alan Davidson, Director of Public Policy, Google Inc.

**Before the U.S. Senate Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety, and Insurance
“Consumer Privacy and Protection in the Mobile Marketplace”**

May 19, 2011

Chairman Pryor, Ranking Member, and Members of the Committee:

I am pleased to appear before you this morning to discuss mobile services, online privacy, and the ways that Google protects our users’ personal information. My name is Alan Davidson, and I am Google’s Director of Public Policy for the Americas. In that capacity, I oversee our public policy operations in the United States, and work closely with our legal, product, and engineering teams to develop and communicate our approach to privacy and security, as well as other issues important to Google and our users.

Google is most well known for our search engine, which is available to Internet users throughout the world. We also make Android, an open operating system for mobile devices that in a few short years has grown from powering one device (introduced in the fall of 2008) to more than 170 devices today, created by 27 manufacturers. We also offer dozens of other popular services, from YouTube to Gmail to Google Earth.

Our business depends on protecting the privacy and security of our users. Without the trust of our users, they will simply switch to competing services, which are always just one click away. For this reason, location sharing on Android devices is strictly opt-in for our users, with clear notice and control. This is the way these services *should* work — with opt-in consent and clear, transparent practices, so consumers can make informed decisions about the location-based services that are so popular.

This is also why we are educating parents and children about online safety, and working with groups like ConnectSafely and Common Sense Media to address the important issues of digital literacy and citizenship, including how to use Google’s privacy, security, and family safety tools.

In my testimony today, I’ll focus on three main points:

- Location-based services provide tremendous consumer benefit;
- Google is committed to the highest standards of privacy protection in our services, as demonstrated in our approach to mobile services, content controls, consumer education, advertising, and security; and
- Congress has an important role in helping companies build trust and create appropriate baseline standards for online privacy and security.

I. Location based services provide tremendous value to consumers

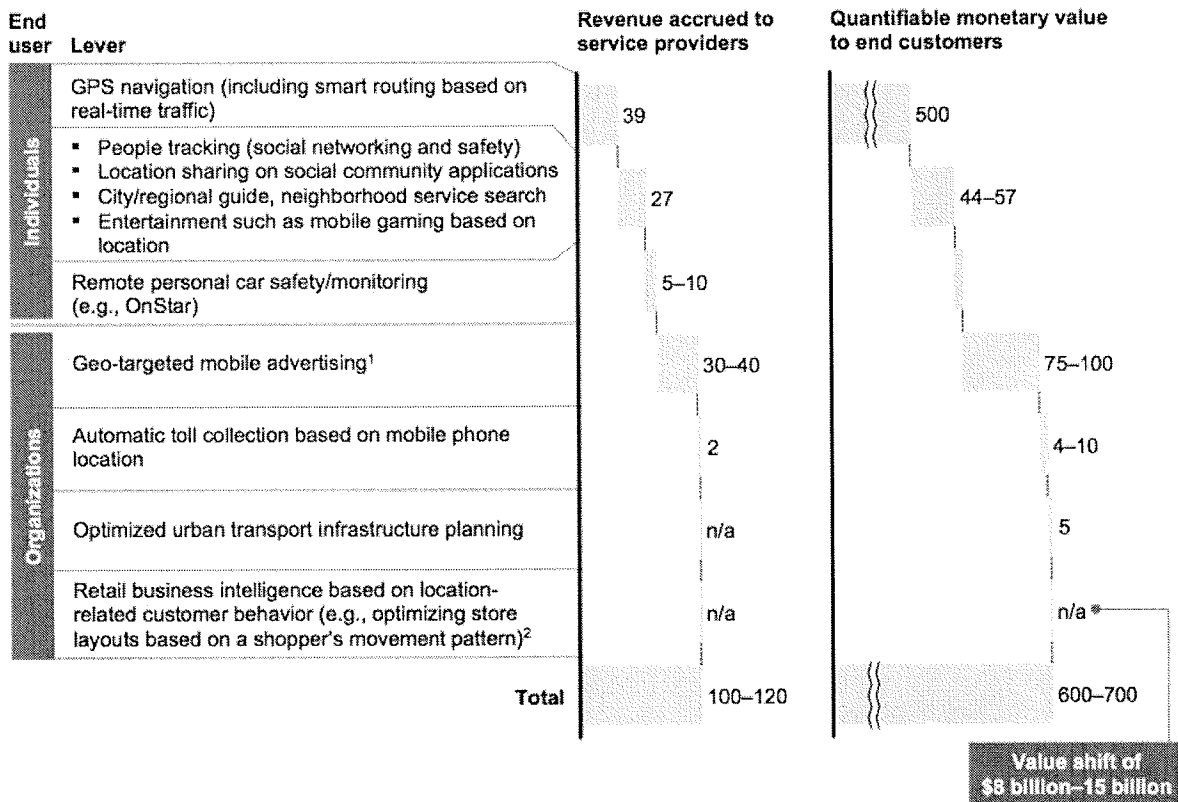
Mobile services are creating enormous economic benefits for our society. A recent market report predicts that the mobile applications market will be worth \$25 billion by 2015. McKinsey estimates that personal location applications will generate as much as \$700 billion in consumer value in the next eight years.

People can use mobile services to get driving directions from their current location, identify a traffic jam and find an alternate route, and look up the next movie time at a nearby theater. Location can even make search results more relevant: If a user searches for “coffee” from a mobile phone, she is more likely to be looking for a nearby café than the Wikipedia entry describing coffee’s history. In the last year, a full 40% of Google Maps usage was from mobile devices. There are now 150 million active monthly Google Maps for Mobile users on Android, iPhone, BlackBerry, and other mobile platforms in more than 100 countries.

Thousands of other organizations and entrepreneurs offer applications that use location services to provide helpful products. For example, the U.S. Postal Service offers an application to help users find nearby post offices and collection boxes, based on their location. If you want a Five Guys burger, their application will find a location for you, and even lets you order in advance. Services such as Yelp and Urbanspoon use location to provide local search results, while applications like Foursquare let users find nearby friends who have chosen to share their location.

The value of the major levers increases to more than \$800 billion by 2020

\$ billion per annum



¹ For sizing the value of geo-targeted mobile advertising, service providers are defined as those that sell advertising inventory, e.g., advertising platform providers; customers are defined as the marketers who purchase advertising inventory.

² Individual retailer will gain top-line increase, which represents a value shift rather than value creation at macro-level.

Source: [McKinsey Global Institute analysis](#)

Mobile location data can even save lives. In crisis situations, people now turn to the Internet to find information. Within a few hours of the Japan earthquake, for example, Google saw a massive spike in search queries originating from Hawaii related to “tsunami.” We placed a location-based alert on the Google homepage for tsunami alerts in the Pacific and ran similar announcements across Google News, Maps, and other services. In cases like the Japanese tsunami or the recent tornadoes in the U.S., a targeted mobile alert from a provider like Google, or from a public enhanced 911 service, may help increase citizens’ chances of getting out of harm’s way.

Other emergency notifications like AMBER alerts can be improved using location data, too. In the past, a parent’s best hope of finding a missing child might have been a picture on a milk carton. Google works with the National Center for Missing and Exploited Children (NCMEC) in an ongoing partnership to develop technology solutions that help them achieve their mission. Today, modern tools and information can make NCMEC’s AMBER alerts more effective and efficient through location-based targeting — within seconds of the first report, an AMBER alert could be distributed to all users within one-mile of the incident. As Ernie

Allen, NCMEC's President and CEO, wrote last week:

Google's contributions to our Missing Child Division have also been significant. Your tools and specialized engineering solutions assist our case managers in the search for missing children. . . . We eagerly await the completed development of the AMBER Alert tool, which will expand the reach and distribution of AMBER alerts to Google users and will surely have enormous potential for widespread dissemination of news about serious child abduction cases. Thank you for your continued efforts to give children the safer lives that they deserve.

None of these services or public safety tools would be possible without the location information that our users share with us and other providers, and without the mobile platforms that help businesses and governments effectively reach their audiences.

II. Google is committed to the highest standards of privacy protection in our services

Google would not be able to offer these services — or help create the economic and social value generated from location data — if we lost the trust of our users. At Google, privacy is something we think about every day across every level of our company. It is both good for our users and critical for our business.

Our privacy principles

Privacy at Google begins with five core principles, which are located and available to the public at www.google.com/corporate/privacy_principles.html:

- Use information to provide our users with valuable products and services.
- Develop products that reflect strong privacy standards and practices.
- Make the collection and use of personal information transparent.
- Give users meaningful choices to protect their privacy.
- Be a responsible steward of the information we hold.

First, as with every aspect of our products, we follow the axiom of “focus on the user and all else will follow.” We are committed to using information only where we can provide value to our users. **We never sell our users' personally identifiable information.** This is simply not our business model.

Second, we aim to build privacy and security into our products and practices from the ground up. From the design phase through launch, we consider a product's impact on our users' privacy. And we don't stop at launch; we continue to innovate and iterate as we learn more from users.

Our last three principles lay out our substantive approach to privacy: We are committed to *transparency*, *user control*, and *security*.

Internal process and controls

Google also reflects these principles in our development process and employee training. As we recently explained, we have begun to implement even stronger internal privacy controls with a focus on people, training, and compliance.

All this process is aimed at ensuring that products match our philosophy and avoid mistakes that jeopardize user trust — like the launch of [Google Buzz](#), which fell short of our standards for transparency and user control. To help make sure we live up to this promise, we entered into a consent decree with the Federal Trade Commission this year, under which we'll receive an independent review of our privacy procedures every two years. In addition, we'll ask users to give us affirmative consent before we change how we share their personal information.

Products reflecting principles: Opt-in location controls on Android

We understand location information is sensitive. So our approach to location data is simple: Opt-in consent and clear notice are required for collection and use of location information on Android.

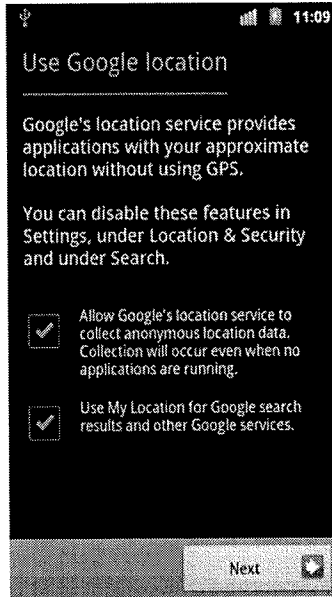
We don't collect any location information — any at all — through our location services on Android devices unless the user specifically chooses to share this information with Google. We also give users clear notice and control; the set-up process explicitly asks users to “allow Google's location service to collect anonymous location data.” And even after the set-up process, users can easily turn off location sharing with Google at any time they wish.

The location services in our Android operating system embody the transparency and control principles that we use to guide our privacy process. We hope that this will be a standard for the industry.

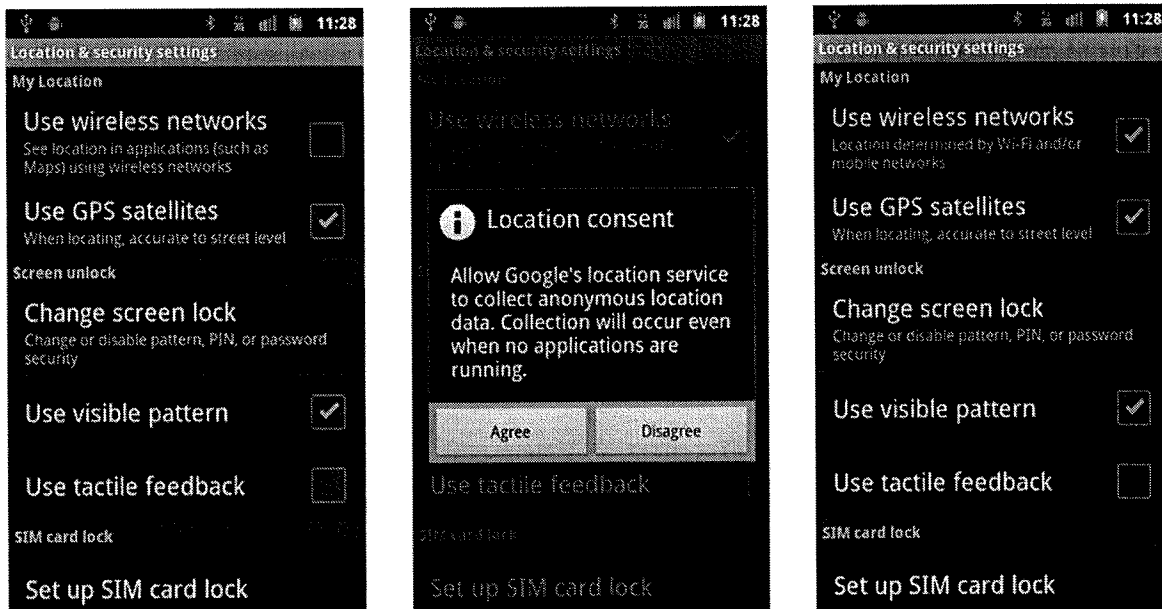
Google is also very careful about how we use and store the data that is generated by these services. The location information sent to Google servers when users opt in to location services on Android is anonymized and stored in the aggregate. It's not tied or traceable to a specific user. The collected information is stored with a hashed version of an anonymous token, and that hashed token is deleted after approximately one week. A small amount of location information regarding nearby Wi-Fi access points and cell towers is kept on the Android device to help the user continue to enjoy the service when no server connection is available and to improve speed and battery life.

In order to provide these location services, many companies detect nearby, publicly available signals from Wi-Fi access points and cell towers and use this data to quickly approximate a rough position, even while they may be working on a more precise GPS-based location. This can be done by using information that is publicly broadcast (for example, that list of Wi-Fi access points you see when you use the “join network” option on your computer). Companies like Skyhook Wireless and Navizon compile such information and license the data to many industry leaders.

Google has a similar location service called the Google Location Server — an Internet database that uses Wi-Fi access points and cell towers to determine an estimated location and that uses GPS information to estimate road traffic. Device manufacturers can license the Network Location Provider application for Android from Google. This Network Location Provider is turned off by default. It can be turned on by the user during the phone's initial setup or in the device settings.



The Network Location Provider is off by default. The user can opt-in and turn on location services during the initial setup flow.



The user can opt-in to turn on the Network Location Provider on their Android phone from within the device settings.

The Android operating system is built on openness, with the goal of encouraging developers to innovate. With this principle in mind, Google does not decide which applications can access location or other user information from the device. Instead, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access. The user

may choose to trust the application by completing the installation or the user may choose to cancel the installation. An application can only access the device's GPS location or the device's network location if it displays a notice for this permission to the user at time of installation.

When Google creates an Android application, like Google Maps for mobile devices, Google is responsible for how the application collects and handles data and for the privacy disclosures made to users, and generally applies the [Google Mobile Terms of Service](#) and the [Google Mobile Privacy Policy](#). These privacy policies are also clearly displayed to the user when the user first signs into the Android device.

When an Android application is not developed by Google, the application developer bears the responsibility for its design and its use of data. Google does not and cannot control the behavior of third party applications, or how they handle location information and other user information that the third party application obtains from the device. Google does strongly encourage application developers to use best practices as described in this [Google blog post](#).

How our products reflect our principles: Parental controls and family safety

While Google does not offer services directed at children, we try to provide families with the tools and education to ensure a positive and safe experience on our services. In addition to our work with NCMEC and others to protect children, our major consumer education initiatives include:

- **Android Market content ratings.** The content rating system is a new feature of Android Market that requires developers to rate their apps in one of four categories, in accordance with our [guidelines](#): Everyone, Low-, Medium-, or High-Maturity. Developers are responsible for rating the apps, and if users come across incorrectly rated apps, they can flag them for review.
- **SafeSearch on Mobile.** Just as with Google Web Search on desktop, Google's SafeSearch filter is accessible on mobile for users who search on a mobile browser. SafeSearch uses advanced technology to block sexually explicit images and text from search results. Users can customize and lock their SafeSearch settings to 'Strict' or 'Moderate' by clicking on the 'Settings' link to the top right corner of the homepage on Google.com.
- **Digital Literacy initiative.** To help educate families about responsible Internet use, we developed a [curriculum](#) with iKeepSafe that teaches teens to recognize online risks, investigate and determine the reliability of websites, and avoid scams. We've sponsored a tour that iKeepSafe is taking across the country to bring the curriculum into local communities and classrooms.
- **Family Safety Center.** In cooperation with the Federal Trade Commission's OnGuardOnline initiative and other child safety advocates and experts, we built a one-stop shop for families, available at www.google.com/familysafety, to provide step-by-step instructions for using safety tools built into Google products and other best practices for families to consider. In response to popular requests, we've added a section about [managing geolocation features on mobile phones](#).
- **Net Safety Tips on the Go app.** The Internet Education Foundation, in partnership with Google and others, [created an app](#) to help users keep up with online privacy, safety, and security issues on your Android phone. It provides quick, practical, friendly advice for you and your family. The tips,

developed by leading online safety organizations, cover important issues like mobile privacy and safety, sexting and cyberbullying, social networking safety, and avoiding identity theft.

How our products reflect our principles: Advertising and privacy

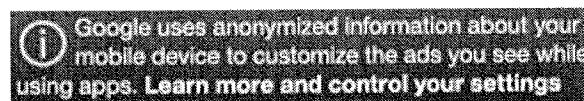
John Wanamaker, considered by some to be the father of modern advertising, once remarked that “half the money I spend on advertising is wasted; the trouble is I don't know which half.” Google’s advertising products are aimed at eliminating that wasted half, bringing data-driven efficiency to advertising. But as we work to bring more relevant and useful ads to our users, we continually seek to preserve transparency and user control over the information used in our ad system.

Google was not the first to offer interest-based advertising (known as IBA) online, but when we launched IBA, in March 2009, we included a number of groundbreaking privacy features. Google’s interest-based ads contain notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads, or to opt-out of interest-based advertising altogether. Note that we do not serve interest-based ads based on sensitive interest categories such as health status or categories relating to kids. We are also participating in the [industry-wide ad targeting notice and opt-out program](#).

We have seen that for every visitor that opts out of IBA on this page, seven users view or edit their settings and choose to remain opted in. We take from this that online users appreciate transparency and control, and become more comfortable with data collection and use when we offer it on their terms and in full view.

Recently, discussions about online ad targeting have centered on the ability of users to indicate a desire to opt out of this profiling and targeting by all online providers — sometimes called Do Not Track. In January, Google sought to further encourage consistency and ease of control over online targeting by launching the [Keep My Opt-Outs](#) Chrome extension, which enables all providers participating in ever-expanding industry self-regulatory programs to make their IBA opt outs *permanent* via a simple browser-based mechanism. As new opt outs come online, we will automatically update this extension to keep users up to date. In the first few months, more than 100,000 users have already installed and are using the extension. We even released this tool on an [open-source](#) basis so that other developers can examine, assess, enhance, or even extend the code’s capabilities. Additionally, we are developing versions of Keep My Opt Outs that work on other major browsers.

Just last month, we extended our advertising privacy approach to our mobile application ad networks. These networks help mobile app developers make money from their products. For these ad systems, we have created a user-friendly solution involving anonymization, user control, and user notice. First, Google performs a one-way, non-reversible hashing of a device identifier to create an anonymous ID specifically for ad serving. Second, for both Android and iPhone users we give consumers an easy way to opt out the use of their device identifier by Google's advertising services altogether. Third, we are notifying all users of how we customize ads and their opt-out controls with clear notice as you see here.



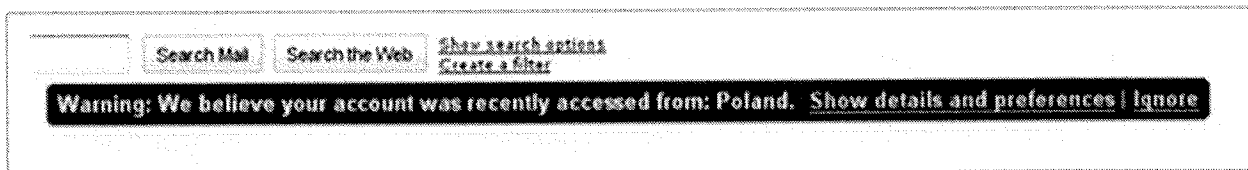
Because the mobile application interfaces are more limited, we chose to rotate full-size privacy notices in with other advertisements, rather than use an icon, which is hard to see or click on the smaller mobile screen.

How our products reflect our principles: Security through encryption and two-step verification

Along with transparency and user control, strong security for users of Google's services to protect against hackers and data breach is vital.

For example, Google was the first (and still only) major webmail provider to offer session-wide secure socket layer (SSL) encryption *by default*. Usually recognized by a web address starting with "https" or by a "lock" icon, SSL encryption is used for online banking and other secure transactions. Users can also encrypt search. Just type "<https://encrypted.google.com>" into your browser to encrypt your search queries and results. We hope other companies will soon join our lead.

In March of last year Google introduced a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail account may have been compromised will be notified and given the opportunity to change her password, protecting herself and her contacts.



Finally, we recently released 2-step verification for consumer Gmail accounts, which allows users who are concerned about the security of their account to use a password plus a unique code generated by a mobile phone to sign in. It's an extra step, but it's one that significantly improves the security of a Google Account. Now, if someone steals or guesses a Gmail user's password, the potential hijacker still cannot sign in to the user's account because the hijacker does not have the user's phone. We are already hearing stories from our users about how this extra layer of security has protected them from phishing attacks or unauthorized access.

III. Congress should act to build trust and create appropriate baseline standards

Congress has a vital role to play in encouraging responsible privacy and security practices, both by bringing attention to these issues and through legislation where appropriate.

The first step Congress can take, and one on which we can all find common ground, is the need for basic "digital citizenship" education for parents, children, teens, and all consumers. Digital skills are essential life skills in a 21st century economy, including understanding basic technical concepts like how to create a safe password and avoid online scams, to critical thinking such as evaluating whether information on a blog is reliable or not. It is crucial that Congress and providers work together to create resources for programs that address these issues and promote them to all consumers, particularly parents and educators.

A second area for careful consideration is legislation. Google supports the development of comprehensive, baseline privacy framework that can ensure broad-based user trust and that will support continued innovation. We salute the work of Senators Kerry and McCain to develop a comprehensive approach to this issue, based on the same principles of transparency, control, and security we apply to our own services. We look forward to continued conversations about this bill as it evolves.

Key considerations for any comprehensive approach to privacy include:

- **Even-handed application.** A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline and online data collection and processing should, where reasonable, involve similar data protection obligations.
- **Recognition of benefits and costs.** As with any regulatory policy, it is appropriate to examine the benefits and costs of legislating in this area, including explicit attention to actual harm to users and compliance costs.
- **Consistency across jurisdictions.** Generally, Internet users neither expect nor want different baseline privacy rules based on the local jurisdiction in which they or the provider reside. Moreover, in many instances, strict compliance with differing privacy protocols would actually diminish consumer privacy, since it would require Internet companies to know where consumers are located at any given time.

By the same token, in general we do not support a continued “siloed” approach to privacy law. While much of today’s debate centers on location information and “Do Not Track” advertising privacy proposals, providers and consumers need a comprehensive approach that will set consistent, baseline principles for these issues and those to come in the future. Otherwise, this Committee and others will be returning term after term to address the latest new technology fad.

Moreover, industry response to the advertising privacy issue has been encouraging. In a few short months, all major browser companies have introduced new controls, and the advertising and online publishing industries have come together to announce uniform standards for notice and control over targeted ads.

We can, however, suggest two concrete areas where Congress can act immediately to strengthen Americans’ privacy protections and provide consistency for providers.

Congress should promote uniform, reasonable security principles, including data breach notification procedures. We pride ourselves at Google for industry-leading security features, including the use of encryption for our search and Gmail services. But we need help from the government to ensure that the bad acts of criminal hackers or inadequate security on the part of other companies does not undermine consumer trust for all services. Moreover, the patchwork of state law in this area leads to confusion and unnecessary cost.

In addition, the Electronic Communications Privacy Act, the U.S. law governing government access to stored communications, is outdated and out of step with what is reasonably expected by those who use cloud computing services. ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today, leaving us in some circumstances with complex and baffling rules that are both difficult to explain to users and difficult to apply.

As part of the [Digital Due Process coalition](#), we are working to address this issue. The Digital Due Process coalition includes members ranging from AT&T to Google to Americans for Tax Reform to the ACLU. It has put forward common sense principles that are designed to update ECPA, while ensuring that government has the legal tools needed to enforce the laws.

Particularly relevant to today's hearing, the coalition seeks to:

- **Create a consistent process for compelled access to data stored online.** Treat private communications and documents stored online the same as if they were stored at home and require a uniform process before compelling a service provider to access and disclose the information.
- **Create a stronger process for compelled access to location information.** Create a clear, strong process with heightened standards for government access to information regarding the location of an individual's mobile device.

Advances in technology rely not just on the smart engineers who create the new services, but also on smart laws that provide the critical legal underpinning for continued innovation and adoption of the technology. We hope to work with this Committee and with Congress as a whole to strengthen these legal protections for individuals and businesses.

* * *

Google appreciates the efforts of this subcommittee to address the critical privacy and security issues facing consumers. We look forward to working with you, and to answering any questions you might have about our efforts.

Thank you.



MOBILE MARKETING ASSOCIATION

Mobile Advertising Guidelines

Version 5.0

Mobile Marketing Association



1.0 Overview 2

2.0 Mobile Web 3

2.1 Mobile Web Advertising Unit Definitions 3

2.2 Mobile Web Banner Ad Specifications 3

2.3 Mobile Web Advertising Content - Creative Design Principles 6

2.4 Mobile Web Advertising Insertion and Delivery 6

3.0 Text Messaging (SMS) 7

3.1 SMS Advertising Unit Definitions 7

3.2 Initial SMS Ad Specifications 7

3.3 Complete SMS Ad (Full Message) Specifications 8

3.4 SMS Advertising Insertion and Delivery 8

3.5 Creative Design Principles 9

4.0 Multimedia Messaging (MMS) 10

4.1 MMS Advertising Unit Definitions 10

4.2 MMS Advertising Unit Specifications 11

4.3 MMS Advertising Creative Design Principles 12

4.4 MMS Advertising Insertion and Delivery 13

5.0 Mobile Video and TV 14

5.1 Mobile Video and TV Advertising Unit Definitions 14

5.2 Mobile Video and TV Ad Break Specifications 15

6.0 Mobile Applications 16

6.1 Mobile Application Advertising Unit Definitions 17

6.2 Mobile Application Advertising Unit Specifications 17

6.3 Mobile Application Advertising Creative Design Principles 18

7.0 Technical Requirements for Mobile Advertisers 20

8.0 Who We Are 20

9.0 References 21

10.0 MMA Guidelines Approval Process 22

11.0 Supporting Associations 23

12.0 Contact Us 23

13.0 Glossary of Terms 23

Appendix 1 – WAP 1.0 Specifications 24

1.0 Overview

The MMA's Mobile Advertising Guidelines provide recommendations for the global ad units generally used in mobile advertising across the following mobile media channels: mobile web, messaging, applications and mobile video and TV¹. The Guidelines recommend ad unit usage best practices, creative technical specifications, as well as giving guidance on ad insertion and delivery. The guidelines are intended to promote the development of advertising on mobile phones by:

- Reducing the effort required to produce creative material,
- Ensuring that advertisements display effectively on the majority of mobile phones
- Ensuring that advertisements provide an engaging, non-intrusive consumer experience.

The MMA guidelines are the result of ongoing collaboration across the MMA Mobile Advertising Committee with representation from companies in Asia Pacific (APAC), Europe, Middle East and Africa (EMEA), Latin America (LATAM) and North America (NA). Committee members are representative of all parties in the mobile marketing ecosystem, including handset manufacturers, operators, content providers, agencies, brands and technology enablers.

The target audience for these guidelines is all companies and individuals involved in the commissioning, creation, distribution and hosting of mobile advertising. The MMA Mobile Advertising Guidelines are designed to establish a common and basic set of standards adopted by all these parties and by doing so both accelerate market development and ensure consumer acceptance.

In addition to the guidelines published below, the MMA also produces a Mobile Advertising Overview. This is a supplemental document that provides an overview of the mobile media channels that are available to advertisers today, as well as the benefits of, and considerations for, optimizing campaign effectiveness and strengthening consumer satisfaction. The Mobile Advertising Overview can be found on the MMA Website at <http://www.mmaglobal.com/mobileadoverview.pdf>

Universal Mobile Ads

The MMA's Mobile Advertising Guidelines are increasingly accepted as best practice across the industry worldwide. In order to make preferred MMA ad units easier to define, adopt and reference, a subset of advertising units have been defined as "universal" mobile ad units. These "universal" mobile ad units already enjoy broad support across the industry. The MMA has summarized those universal ad units in their "Universal Mobile Ad Package", which can be found on the MMA website at <http://www.mmaglobal.com/umap.pdf>.

Publishers who are compliant with the MMA Mobile Advertising Guidelines will accept advertisers who provide at least one of the ad units designated "universal" in this document, and will attest that these ad units have the ability to reach the majority of that publisher's audience. Publishers are, of course, also free to offer more ad units beyond universal units.

Advertisers can be sure that by producing creative material according to these universal ad units, they will be able to advertise through publishers who are compliant with the MMA Mobile Advertising Guidelines. Advertisers are not obliged to provide all ad units in every case. Also, advertisers are free to use ad units beyond those defined as universal.

¹ This document provides recommendations and specifications for the generic Mobile Advertising formats that are accepted widely across the industry. Proprietary systems and technologies that are used by singular providers such as iAd from Apple are not covered by this document.

2.0 Mobile Web

This section provides recommendations for the most prevalent advertising units on the Mobile Web, graphical banner advertising and text links.

The Mobile Web features text and graphics optimized to match the specific screen resolutions and browser capabilities of each user's mobile phone. A smartphone with a high resolution screen is capable of handling larger, more visually rich ads than a legacy mobile phone with fewer resources, which can only be served light-weight ads designed for small screens with limited resolution.

In order to accommodate the wide range of mobile phone capabilities, it is recommended that advertisers produce and provide ad creative in a few of the pre-defined dimensions discussed in this section. By doing so, advertisers can ensure that the ad unit is matched to the mobile phone model's capabilities, and that it best fits the mobile phone's display. This approach helps ensure a good user experience and increases process and campaign effectiveness.

2.1 Mobile Web Advertising Unit Definitions

The recommended ad units for Mobile Web are as follows:







- **Mobile Web Banner Ad** is a universal color graphics ad unit displayed on a Mobile Web site. The universal Mobile Web Banner Ad is defined as a still image intended for use in mass-market campaigns where the goal is a good user experience across all mobile phone models, network technologies and data bandwidths. In some cases animated mobile web ad banners may be available for supplemental use in campaigns to convey a richer experience. All Mobile Web Banner Ads must be clickable by the end user and may be placed in any location on a Mobile Web site. A Mobile Web Banner Ad may be followed by a Text Tagline Ad to emphasize the clickable character of the ad unit.
- **Rich Media Mobile Ad (RMMA)** is a supplemental ad unit defined by the two-stage principle of *display* and *activation*. *Display* is the way an RMMA ad resides in a usual ad space of a host property (application or website) and calls for action in form of a banner or similar ad unit. Only when the user interacts with the displayed banner by clicking or swiping it, do the RMMA features become *activated*, showcasing their characteristic "rich" behavior. Respective guidelines are in advanced stages of development and expected to be added in future releases of this document. Draft RMMA Guidelines are available here: <http://www.mmaglobal.com/rmma.pdf>.
- **WAP 1.0 Banner Ad** is a supplemental black-and-white, still graphics ad unit for use in campaigns that target older mobile phones. A WAP 1.0 Banner Ad can be followed by a supplemental Text Tagline Ad to emphasize the clickable character of the ad unit.
- **Text Tagline Ad** is a supplemental ad unit displaying only text. Text links may be used below a Mobile Web Banner Ad to emphasize the clickable character of the ad unit. Text links may also be used in older mobile phones not capable of supporting graphical images and/or by publishers that prefer to use text ads instead of graphical ads on their mobile sites.




2.2 Mobile Web Banner Ad Specifications

The recommended specifications for Mobile Web ad units cover all important design & build components, i.e. aspect ratios, media formats, dimensions and file sizes. When providing inventory specifications, publishers should remember to specifically quantify the parameters they support for each component.

Table 1 provides a summary of Mobile Web Banner ad unit specifications and examples. Every publisher should support at least one of the universal Mobile Web Banners ad units specified in the table below.

Table 1: MMA Mobile Web Ad Guidelines
Mobile Web Banner Ad Units

Name	Technical Specifications	Sample Creative (approx. dimension)
XX-Large Image Banner	<ul style="list-style-type: none"> • 320 x 50 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 10 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 15 KB file size 	
X-Large Image Banner	<ul style="list-style-type: none"> • 300 x 50 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 10 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 15 KB file size 	
X-Large High Image Banner	<ul style="list-style-type: none"> • 300 x 75 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 10 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • <15 KB file size 	
Large Image Banner	<ul style="list-style-type: none"> • 216 x 36 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 6 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 9 KB file size 	
Large High Image Banner	<ul style="list-style-type: none"> • 216 x 54 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 6 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 9 KB file size 	
Medium Image Banner	<ul style="list-style-type: none"> • 168 x 28 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 4 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 6 KB file size 	

<p>Medium High Image Banner</p>	<ul style="list-style-type: none"> • 168 x 42 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 4 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 6 KB file size 	
<p>Small Image Banner</p>	<ul style="list-style-type: none"> • 120 x 20 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 2 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 3 KB file size 	
<p>Small High Image Banner</p>	<ul style="list-style-type: none"> • 120 x 30 pixels <p>Universal unit:</p> <ul style="list-style-type: none"> • GIF, PNG, JPEG for still image • < 2 KB file size <p>Supplemental unit:</p> <ul style="list-style-type: none"> • Animated GIF for animation • < 3 KB file size 	
<p>Text Tagline (optional)</p>	<ul style="list-style-type: none"> • Up to 24 characters for X-Large • Up to 18 characters for Large • Up to 12 characters for Medium • Up to 10 characters for Small • Not used for XX-Large 	<p>Show Times Click Here</p>

Specification Components

2.2.1 Dimensions See Table 1. Establishing guidelines for Mobile Ad unit dimensions has several benefits:

- Limiting the amount of distinct dimensions reduces the amount of time and resources spent on creative production.
- The Dimensions selected have been carefully chosen to provide a good fit for the majority of mobile phones.

2.2.2 Media Formats The recommended formats for Mobile Web Banner Ads are:

- GIF, PNG or JPEG as universal formats for still images.
- GIF for animated images.

2.2.3 File Size The maximum graphic file size is dependent on the size of banner chosen. Table 1 provides the maximum file size recommendations across all of the banner ad units sizes.

Character Limits for Text Taglines Character limits (rather than file size limits) are applicable for Text Taglines appended to Mobile Web Banner Ads. Screen width has no effect on text tagline sizes, which Table 1 summarizes.

WAP 1.0 Banner Ad Specifications Appendix 1 provides a summarization of WAP 1.0 ad specifications. This ad unit is still in use in some markets, however, its importance, overall, is decreasing.

2.3 Mobile Web Advertising Content - Creative Design Principles

In addition to the MMA Mobile Advertising Guidelines, other established guidelines for Mobile Web content delivery should apply to Mobile Web sites containing image banners, as well as to Mobile Web sites that users reach via links in image banners (post-click), such as jump pages, campaign sites and self-contained, permanent third-party Mobile Web sites.

More detailed design principles and style guides for Mobile Web sites can be found in the W3C Mobile Web Best Practices at <http://www.w3.org/TR/mobile-bp>. The MMA Mobile Advertising Committees also recommends that Mobile Web sites conform to W3C mobileOK Basic 1.0 Guidelines, which are available at <http://www.w3.org/TR/mobileOK-basic10-tests>.

The MMA recommends that advertisements contain some form of call-to-action clearly identifiable by the user (e.g., “find out more” icon button). This is not only sensible from a user experience perspective but also greatly increases the clickthrough rate.

Text Taglines

Text taglines are a supplemental feature that should be added to most Mobile Web Banner Ads where possible.

Purpose:

- Some consumers are unfamiliar with Mobile Web Banner Ads and may not realize that these can be navigated to and clicked on. A Mobile Web Banner Ad with a text tagline may generate higher click rates.
- Some older browsers cannot navigate graphical elements at all. In those cases, a text tagline is required to make the Mobile Web Banner Ad clickable.

Note:

- Mobile Web Banner Ads with text taglines will use more real estate (space in the usable browser window), typically at the expense of other Web elements, such as navigation and content.

2.4 Mobile Web Advertising Insertion and Delivery

The following recommendations are for Mobile Web advertising insertion and delivery, as appropriate to the technology.

2.4.1 Ad Indicators

Some publishers and markets recommend or require the use of ad indicators (signifiers) when displaying an ad unit. The publisher or local market guidelines define the exact format and placement of the ad indicator. Indicators are used with both text and banner ads:

- A Text link ad indicator is defined as text used to indicate the text link is an ad. An example is the use of “Ad:” preceding the ad text link.
- A Banner ad indicator is defined as a portion of the Mobile Web Banner Ad used to display the ad indicator and indicate the Mobile Web Banner Ad is an ad unit rather than content. The indicator typically is located on the side or the corner of the ad unit and may use text (e.g., “AD” in English speaking markets or “Anzeige” or “-w-“ in Germany) or an icon.

The Mobile Web Banner ad unit specifications in Section 2.1 are inclusive of the ad indicator. When choosing to use an ad indicator, the MMA recommends that the ad indicator be included within the creative build.

2.4.2 Functionality

Automatic resizing of Mobile Web banners

Some publishers and ad-serving solutions provide a capability to re-size the ad creative dynamically to match the mobile phone's screen dimensions and capabilities.

In cases where the publisher or ad-serving solution requires only one banner image, the MMA recommends using the X-Large Mobile Web Banner ad unit specifications as the default re-sizeable banner. It's important that the creative takes into account both the impact of image re-sizing (i.e. certain amount of degradation of image quality) and that the automatic resizing may not work well with animated banners.

Animated banner images

When using animated Mobile Web Banner Ads, please note:

- Mobile phones that don't support image animation tend to render only the first image frame. For this reason, the MMA recommends that the first image frame should contain the entire advertising message, instead of leaving important information for subsequent frames.
- To date, automatic resizing of animated images does not always deliver ideal results. Therefore, the MMA does not recommend applying automatic resizing with animated image banners. The MMA is studying this issue in order to find a workable recommendation.
- There are several possible animation formats, including animated GIF, SVG, Flash, Silverlight and interlaced JPEG. Animated GIF currently is the most widely supported on mobile phones. The MMA is studying options for improvements that will be incorporated into future guidelines.

3.0 Text Messaging (SMS)

Short Message Service (SMS) is a communications service that allows the exchange of short text messages, limited to 160 characters, between mobile phones. It is also referred to as "text messaging" or "texting." SMS messages can be sent and received between virtually all operator networks. Virtually every mobile phone in the world supports SMS, creating a ubiquitous market for SMS-based advertising campaigns. SMS supports messages sent from one user to another, as well as messages sent from a machine, such as a PC, application or server, to a user.

3.1 SMS Advertising Unit Definitions

The recommended ad units for SMS are as follows:

- **Initial SMS Ad (Appended)** is a universal text ad unit of variable length (often between 20-60 characters) appended to the content (or body) portion of the message containing the primary, non-advertising content of the message. This ad unit uses the remaining space after the content portion of the message, and can be made available for advertiser usage by the publisher. As a principle, focus should remain on the content portion which should not be compromised by the ad unit.
- **Complete SMS Ad (Full Message)** is a universal text ad unit with up to 160 characters available for advertiser usage. There is no primary, non-advertising content in the message and this ad unit is typically delivered as a reply to an Initial SMS Ad or "Text (keyword) to (short code)" call-to-action. These ads may be delivered as part of an ongoing opt-in mobile advertising campaign.

3.2 Initial SMS Ad Specifications

Specification Components

3.2.1 Format SMS is a text-only medium. It does not support any rich media; however some mobile phones with click-to-call or click-to-web capability will display colored links and underlining of URLs and phone numbers. The font size is entirely controlled by the mobile phone and is not under the control of advertiser or publisher. Therefore the message renders differently on different mobile phones.

3.2.2 Length The length of the ad is subject to the space available after the content. Consult your publisher for the maximum allowable length. Current best practice is for ads to be no shorter than 20 and no longer than 90 characters in length. Advertisers should be aware that by using shorter copy they increase the likelihood of availability of publisher inventory.

When using double-byte characters (otherwise known as 16-bit) to send an SMS, the limit is 70 characters. 16-bit characters are associated with sending a Unicode text message, which is required to convey some of the special characters used in non-Latin alphabets, such as Chinese, Japanese or Korean.

3.2.3 Location The ad copy will be inserted only at the end of the content portion of the SMS. In cases where the sender uses a personal SMS signature, the ad should be inserted after the signature.

3.3 Complete SMS Ad (Full Message) Specifications

Specification Components

3.3.1 Format SMS is a text-only medium. It does not support any rich media; however some mobile phones with click-to-call or click-to-web capability will display colored links and underlining of URLs and phone numbers. The font size is entirely controlled by the mobile phone and is not under control of the advertiser or publisher. Therefore the message renders differently on different mobile phones.

3.3.2 Length A length of up to 160 Latin characters

3.3.3 Location The SMS message is entirely devoted to the advertisement.

3.4 SMS Advertising Insertion and Delivery

3.4.1 SMS Ad Indicators

The publisher or advertising insertion partner is responsible for including an ad indicator in Initial (Appended) SMS Ads. There should be a clear separation between the text message content and the ad. A carriage return or line break is recommended, however not all carriers support line breaks, so an ad indicator should also precede the ad copy. Acceptable ad indicators are:

- "*" (single asterisk)
- "**" (double-asterisk)
- "AD:" (or similar local language abbreviation)
- "-" (dash)

Note that a carriage return may count as two characters.

3.4.2 SMS Ad Functionality

Delivery

- Delivery of SMS Ad messages should be consistent with the MMA Global Code of Conduct. In the U.S., SMS Ad messages should also follow the MMA Consumer Best Practice Guidelines: <http://www.mmaglobal.com/bestpractices.pdf>

Response (return SMS)

- If a user requests additional information be delivered to them via SMS, advertisers should respond to that request within 12 hours or the request (opt-in) for that particular message will be deemed expired.
- Responses to user requests may be delivered by an alternate common short code or phone number, but the relationship to the original request should be clearly identifiable by the user. (For more information about short codes, see the MMA *Common Short Code Primer*, available at <http://www.mmaglobal.com/shortcodeprimer.pdf>)

Click-to-call

- Phone numbers should be local or domestic to the country that the ads are targeting.
- Phone numbers should be functional. Ensure that the numbers are in service before the campaign launches.
- Premium destination numbers that would result in a charge that exceeds standard rates to the end user should not be used unless the terms are fully disclosed in the ad.
- Emergency numbers (e.g., 911 in the United States and Canada, or 112 in parts of Europe), or any unrelated service numbers, are not allowed in SMS ad units.

Link to Mobile Web site

- The advertiser landing page should be viewable in Mobile Web browsers.
- The content of the advertiser landing page should be related to the advertisement.
- The advertiser landing page should be working properly.
- Please see Section 2.3 of this document for best practice around mobile web advertising content.

3.5 Creative Design Principles

The primary design goal should be that the SMS Advertising unit is clearly identifiable as an advertisement and is easily understood by the receiver of the message. The following design principles are suggestions towards achieving the goal of understandability and transparency.

3.5.1 General Design Principles for SMS Ads

- Use abbreviations and “text speak” (e.g., LOL) with caution and avoid grammatical errors or misunderstandings.
- Use punctuation when required for clarity or emphasis.
- Note that a carriage return may count as two characters.
- Conduct testing to ensure that the publishing network recognizes, and mobile phones properly render, any non-Latin or accented letters prior to use.
- Note that URLs contained in the text may allow click through to Mobile Web pages, depending on handset capability, and may appear underlined or in color.

3.5.2 Design Principles for Initial SMS (Appended) Ads

- If a URL is included in an appended ad, the URL should be as short as possible. A URL under 20-characters is recommended.
- To optimize the potential for frequency of delivery, the advertiser should develop several versions of ads of varying character lengths, thus maximizing the advertisements’ availability for insertion alongside non-advertising content of varying lengths For example, “Nike” or “Just do it - Nike.”

3.5.3 Design Principles for Complete SMS (Full Message) Ads

- The Complete SMS Ad unit can be used for any type of promotional message or call to action.
- The advertiser should be clearly identified in the ad copy.

- Creative may contain a URL. Use of short URLs is recommended to use reduce character count and maximize clarity and use of advertising space.
- The title or header of the message should reflect the consumer query or subscription that resulted in delivery of the full ad message copy. For example, if the consumer replied “HOME” to get more info on real estate, the resulting ad should have “HOME” in the first line. This is to avoid user confusion over the source of the ad.

4.0 Multimedia Messaging (MMS)

Multimedia Messaging Service (MMS) is a rich media messaging service that allows mobile users to send and receive messages/media that can include graphics, photos, audio, video and text. Unlike the Mobile Web, this media resides on the user’s mobile phone, so a data connection isn’t required to access the ad content once the message has been received. MMS is not yet universally supported by all operator networks and all mobile phones; however the advertising opportunity using MMS is significant.

These guidelines seek to ensure a clear distinction of MMS Advertising units from content to avoid the perception of MMS Advertising as unsolicited communication and to ensure maximum ad campaign effectiveness.

The MMS guidelines consist of a set of ad unit dimensions, file formats and maximum file sizes, as well as additional considerations for advertisers and publishers.

4.1 MMS Advertising Unit Definitions

The recommended ad units for MMS are as follows:

- **MMS Short Text Ad** is a supplementary text ad unit appended to the content (or body) portion of an MMS slide containing the primary, non-advertising content of the MMS slide. A MMS Short Text Ad can contain links that are clickable by the end user. As a principle, focus should remain on the content portion of the MMS slide which should not be compromised by the ad unit.
- **MMS Long Text Ad** is a supplementary text ad unit filling all of an MMS slide, whereby the text can contain a link that is clickable by the end user.
- **MMS Banner Ad** is a supplementary color graphics ad unit displayed at the top or bottom of an MMS slide. The supplementary MMS Banner Ad is defined as a still image intended for use in mass-market campaigns where the goal is a good user experience across all mobile phone models, network technologies and data bandwidths. However, in some cases, particularly in Europe, supplementary animated MMS Banner Ads are available for use in campaigns where it is imperative to convey a richer experience. An MMS Banner Ad can be clickable by the end user, in which case a separate text link can be considered. The MMS Banner Ad unit specification is similar to the Mobile Web Banner Ad specification in terms of dimension.
- **MMS Rectangle Ad** is a universal color graphics file plus optional text ad unit filling all of an MMS slide. The universal MMS Rectangle Ad is defined as a still image intended for use in mass-market campaigns where the goal is a good user experience across all mobile phone models, network technologies and data bandwidths. However, in some cases, particularly in Europe, supplemental animated MMS Rectangle Ads are available for use in campaigns where it is imperative to convey a richer experience. An MMS Rectangle Ad can be clickable by the end user, in which case a separate text link below the graphics is recommended. An MMS Rectangle Ad can be placed before the original content (pre-roll), within (mid-roll) or after (post-roll) of the MMS, on a separate slide. Mixing an MMS Rectangle Ad with other content (except audio) on one slide is not recommended.
- **MMS Audio Ad** is a supplementary audio clip that is played while an MMS Rectangle Ad or an MMS Full Ad is displayed.

- **MMS Video Ad** is a supplementary video ad unit which is usually delivered as part of a MMS Full Ad.
- **MMS Full Ad** is a supplementary ad unit which only contains advertising content. The MMS Full Ad is a complete MMS composed of elements of MMS Short Text Ads, MMS Long Text Ads, MMS Banner Ads, MMS Rectangle Ads, MMS Audio Ads and MMS Video Ads and distributed over one or multiple slides. There is no primary, non-advertising content in the MMS Full Ad and this ad unit is typically delivered in response to an ad request or based on some form of valid consent (opt-in) provided by the recipient.

4.2 MMS Advertising Unit Specifications

Specification Components

The following ad unit specifications provide the framework for producing MMS ad creative material suitable across a broad range of mobile phones and which offers a compelling and engaging user experience.

4.2.1 Media Formats for MMS ad units are as follows:

- JPG or GIF as universal formats for still images.
- GIF for animated images.
- AMR-NB (on GSM networks) and QCELP (on CDMA networks) are prevailing audio formats.
- AAC+, AAC, MP3, WAV (PCM encoded) are increasingly available on mobile phones.
- 3GP and 3G2 are the prevailing video formats. Recommended audio quality: @ 16bit 44 KHz Stereo; Recommended video quality: QVGA @250kbps, 20-30 frames per second.

4.2.2 Dimensions

For all graphical MMS Ad elements, widths & heights are recommended as defined for the Mobile Web Banner Ad units in Section 2.2, i.e.

- XX-Large MMS Image (width 320 pixels)
- X-Large MMS Image (width 300 pixels)
- Large MMS Image (width 216 pixels)
- Medium MMS Image (width 168 pixels)
- Small MMS Image (width 120 pixels)

The **Large MMS Image width (216 pixels)** is the universal dimension recommended for use in MMS Ad campaigns where only one dimension is used. This width has proven to produce satisfactory user experience across modern mobile phones in mature mobile markets, such as found in the USA or Europe.

For all MMS Video Ad elements, the following are the most common examples of frequently used dimensions:

- Large MMS Video (320 x 240 pixels)
- Medium MMS Video (176 x 144 pixels)
- Small MMS Video (128 x 96 pixels)

4.2.3 File Size

The maximum MMS message file size available for advertisements depends on the following factors:

- Mobile phones are currently capable of receiving MMS messages between a maximum of 100 KB to 600 KB sizes².

² The number of mobile phones supporting less than 300 KB maximum MMS size is decreasing.

- Mobile network configurations apply irrespective of the mobile phone capability. Currently most networks support a maximum of 300 KB. However, some networks have already increased this limit to 600 KB.

In order to reach a broad audience, the MMA recommends that the complete MMS file size does not currently exceed 300 KB. Maximum MMS file size and maximum ad file sizes are inclusive of all applicable elements (e.g., graphics, text and audio³).

- For ads inserted to other content, the MMS ad file size should not exceed 100 KB. This limit allows 200 KB or more for the original content. This file size allows for good quality MMS Rectangle Ad images, even for many animated images.
- For the MMS Full Ad unit, a maximum file size of 300 KB is recommended.

4.3 MMS Advertising Creative Design Principles

4.3.1 Sender identification

The sender of the MMS Full Ad message should be clearly identifiable by the message recipient. The “from” and “subject” field as well as the first message slide should reflect the consumer request or opt-in context that resulted in delivery of the full ad. The message subject field alone is not sufficient for carrying this information because it is not shown on many mobile phones.⁴

For example, if the consumer has opted in to receiving advertisements from brand XYZ, the full ad messages delivered should have “XYZ” not only in the “from” and “subject” field but also in the first element (text or graphic) of the first slide. Local market guidelines or regulation may also be in place requesting sender identification placement.

4.3.2 Ad Indicators

Advertisers should consult their publisher and local markets to determine requirements for ad indicators. Indicators could be used with both text and graphical ads:

- Text ad indicators, where text is used to indicate the text is an ad. An example is the use of “Ad:” preceding the ad text. See also Section 3.4.1 on SMS ad indicators for more guidance.
- Graphical ad indicators, where a part of the creative is used to display the ad indicator and thus make it clear that the graphic is an ad rather than content. The indicator typically is located on the side or the corner of the creative and may use text (e.g., “AD” in English speaking markets or “Anzeige” or “-w-“ in Germany) or an icon to indicate that the image is an ad.

The ad indicator is part of the graphical and text ad elements as per the technical specifications in Section 4.2. The MMA recommends that when advertisers choose to use an ad indicator, it should be included with the creative material. Conventions for ad indicators vary by market and publisher.

4.3.3 Illustrations

The following example seeks to illustrate a possible pre-roll design.

³ In case of using SMIL, about 1 KB of formatting information should be considered part of the MMS size.

⁴ Please reference the MMA Global Code of Conduct: <http://www.mmaglobal.com/codeofconduct.pdf>

Example 1: MMS Pre Roll



Key elements are:

- ← Announce the service
- ← Clearly distinguish publisher brand from advertisement
- ← Inform customer that the content message will display on the following slide(s)

4.4 MMS Advertising Insertion and Delivery

4.4.1 Impact of Transcoding and Rendering of media on mobile phones

MMS Message delivery includes two steps, transcoding and rendering; both which potentially impact the quality of the message, its formats, and the resolution of media elements.

Many mobile operators support transcoding, also known as media adaptation. Transcoding, which automatically adapts content during message delivery, is done according to the receiving mobile phone capabilities (e.g. screen resolution, maximum message file size, supported media formats) to avoid negative user experience. While transcoding ensures that advertisements (along with possible other content) are consistently presented on all mobile phones, it can have a negative impact on the audio and visual elements if applied extensively. The ad unit specifications as defined in chapter 4.1 seek to reduce the need for transcoding, and retain the quality of the ad creative.

Transcoding and rendering have advantages that are relevant for the purpose of MMS advertising:

- To provide a good experience for users on almost all MMS-capable mobile phones.
- To allow creative material to be provided in one version only.

However, some caution is recommended:

- Image creative should be chosen that properly resizes down to lower resolutions. For example, tiny text and graphical details should be avoided.
- Extensive media adaptation (from very large graphics down to very small ones) may render some creative material a poor quality when shown on low-resolution mobile phone screens. This can happen to graphics containing text, details, thin lines or color palettes with texture.
- Creative producers are recommended to contact MMS service providers and/or network operators for more details. In case transcoding is not available on a network, only the standard audio formats (AMR-NB on GSM networks and QCELP on CDMA networks) are recommended in MMS advertising^{5,6}.

⁵ For GSM networks: http://www.openmobilealliance.org/Technical/release_program/docs/MMS/V1_3-20080128-C/OMA-TS-MMS-CONF-V1_3-20080128-C.pdf

The process of MMS delivery can influence the content of MMS, therefore; testing the impact of resizing on quality and legibility of the creative material is recommended. The MMA further recommends that MMS ad delivery be tested on real phones prior to any campaign execution.

4.4.2 Synchronized Multimedia Integration Language (SMIL)

For MMS messages, SMIL defines the order of images and text on a slide, the time a slide is displayed, and other parameters. Media creators should consider the following SMIL parameters:

- **Region** – defines the order of text and graphics on MMS slides. It determines whether all slides of an MMS will start with graphics followed by text or vice versa. Without this parameter it is up to the MMS client to set the order of image and text on one slide, which may lead to an unfavorable display representation.
- **Height** – determines the percentage of display space reserved for text and graphics respectively; this enables forcing the display of text below a picture in the visible area of the mobile phone display.
- **Duration (dur)** – controls the duration of display for each individual slide of the MMS. This parameter is of importance to synchronize the duration of slide display and length of audio play measured in seconds. If not properly set, the slide show may progress to the next slide before the audio (or video) has finished playing.

4.4.3 Other Considerations

International Roaming

Inserting ads into MMS messages sent to users who are roaming abroad can generate additional user costs because mobile network operators typically charge roaming fees for MMS data usage. The industry is still developing best practices for this situation. Some MMS service providers/operators provide the ability to block ad injection and sending of ad MMS messages to roaming users, thus ensuring a good customer experience. If possible, this option should be used.

Response timing (return MMS)

If a user requests advertising information to be delivered to him via MMS, this request should be responded to within 12 hours or the request (opt-in) for that particular message will be deemed expired.

MMS Video Ads

Advertisers should consider the following when developing MMS Video Ads:

- Avoid using fast-moving videos
- Avoid rapid scene changes (many scene changes in a short period)
- Avoid using small letters for advertising messages

For further considerations, please refer to the Mobile Video and TV Advertising Creative Design Principles in Section 5.2.

5.0 Mobile Video and TV

This section provides recommendations for the most prevalent advertising units used in Mobile Video and TV.

5.1 Mobile Video and TV Advertising Unit Definitions

The recommended ad units for Mobile Video and TV are described as follows:

⁶ The MMA recommends to extend the capabilities of MMS audio composition tools to include the mandatory formats as defined in the standards

Ad Breaks are video or still/animated image advertisements rendered before, during or after streamed or downloaded Mobile Video and TV content.

Linear Ad Breaks take over the full mobile display screen and replace the streamed or downloaded video content for a given period of time. Ad unit formats include:

- **Billboard Ad** – a static image or brand logo typically displayed full screen before or after the video content
- **Bumper Ad** – a short video advertisement or sponsorship indent typically shown before or after the video content
- **Pre-Roll Ad** – a video advertisement shown prior to the video content
- **Mid-Roll Ad** – a video advertisement appearing as a break during the video content
- **Post-Roll Ad** – a video advertisement shown after the video content has ended
- **Book Ending Ad** – a Pre-roll video advertisement with a corresponding bumper ad from the same ad campaign appearing at the end of the video content

Non-Linear Ad Breaks share the mobile display with the streamed or downloaded video content for a given period of time. Ad unit formats include:

- **Overlay Ads** are still/animated image advertisements that appear over the top of video content during playback. These ads can be semi-transparent or opaque and can be shown for the full or partial duration of the video content (appear/disappear effect). Variations include horizontal or vertical promotion banners, sponsorship skins (picture frames) and ad bugs.
- **Companion Ads** are still/animated image advertisements that appear adjacent to video content during playback. Variations include drop-down horizontal banners or L-shaped banners that surround a resized video (shrink and surround).

Interactive Mobile Video and TV Ads are advertisements that allow for user interaction including clicking, browsing, zooming. Guidelines for these types of Mobile TV and Video advertisements are still being researched by the MMA but may include click-to-web, click-to-call, click-to-SMS, click-to-video, click-to-download, click-to-locate, click-to-ad etc.

5.2 Mobile Video and TV Ad Break Specifications

5.2.1 Aspect Ratios

Although most handset display screens have a portrait format, Mobile Video and TV content is typically created and rendered in a landscape format. Recommended landscape aspect ratios for Mobile Video and TV content are 4:3, 16:9 and 11:9.

5.2.2 Ad Placement and Length

Shorter ad break durations of up to 20 seconds are recommended for short form video content of 3 to 5 minutes in length. Longer form video content over 5 minutes may support ad breaks of 30 seconds or more but should be considered in consultation with the content publisher to ensure the best consumer viewing experience.

Table 3: Mobile TV and Video Ad Breaks		
Design Model	Advertisement Placement	Recommended Length
Bumper/Billboard	Before or after content	5 seconds or less.
Pre-Roll only	Before content	Typically 15 seconds.

		30 seconds or less
Mid-Roll only	During content	Typically 15 seconds. 30 seconds or less
Post-Roll only	After content	Typically 15 seconds. 30 seconds or less
Book Ending	Before and after content	Typically 15 seconds. 30 seconds or less

5.2.3 Video/ TV Ad Lengths Exceptions

Video downloads: Video downloads: The total file size of a downloadable video is important, especially for consumers downloading over 2G connections. To minimize the consumer download delay it's important that the playback time of a video is between 30 secs and a maximum of 2 minutes in length. For the longer of these length videos, the MMA suggests shorter pre-rolls and/or a short bumper or vice versa to help minimize file size.

Broadcast TV: Mobile TV is still nascent, so more research is necessary to ascertain consumer preferences regarding advertising lengths within mobile TV. "Traditional" TV ad breaks are long (several minutes) and advertisement lengths should be reviewed with the publisher to ensure good consumer experience.

5.2.4 Media Formats

The recommended formats and resolutions for Mobile Video and TV ad units are:

- Video Ad Specifications (e.g. Pre-Roll Video Ad):
- File formats: WMV, AVI, MOV, MPEG2, .3GP
- Resolution/Aspect Ratio: QVGA, CIF, QCIF
- Recommended audio quality: 16bit 44Khz stereo
- Recommended video quality: 250kbps, 20-30 frames per second

Image Ad Specifications (e.g. Billboard Ad):

- File formats: .JPG, .PNG

Mobile Video and TV Advertising Creative Design Principles

Advertisers should consider the following when developing mobile video/TV campaigns:

- Avoid using fast-moving videos
- Avoid rapid scene changes (many scene changes in a short period)
- Avoid using small letters for advertising messages
- Avoid dark shots
- Consider shooting made-for-mobile versions of commercials

Existing video advertising creative assets that have been shot for TV or online may not be optimal for mobile and could need re-editing. For instance, text may be difficult to read, and fast-moving action that is too far into the distance may not be visible or look good on the mobile screen.

6.0 Mobile Applications

This section addresses advertising guidelines for applications that host ads inside the application design and logic. Specifications

Future: Location Based Advertising

The MMA recognizes the need to provide guidelines for location based advertising. However, models for using location currently vary, and do not allow identification of the most appropriate guidelines at this point in time. MMA's mobile advertising committee has started exploring the opportunities of using location in advertising and plans to come up with guidelines for location based advertising. In the meantime, MMA encourages experimentation in this space and invites companies to share best practice with the MMA mobile advertising committee.

presented here are applicable to a wide range of application types comprising managed platforms, virtual machines, native applications and widgets. There are however applications that may not be able to make use of these guidelines (e.g. ad units within idle screen applications). These types of applications will be addressed in future releases of these guidelines. For a more comprehensive overview of the mobile applications landscape, please consult chapter 4.0 of MMA's Mobile Advertising Overview document

(<http://www.mmaglobal.com/mobileadoverview.pdf>).

6.1 Mobile Application Advertising Unit Definitions

The recommended ad units for Mobile Applications are as follows:

- **In-App Display Advertising Units**

Mobile Application Banner Ad – is a universal color graphics ad unit displayed on a Mobile Application. The universal Mobile Application Banner Ad is defined as a still image(s), text or combination of these intended for use in mass-market campaigns where the goal is a good user experience across all mobile phone models, network technologies and data bandwidths. A Mobile Application Banner Ad can be clickable by the end user and may be placed anywhere in a Mobile Application (e.g., on the application main menu page, subpages or content pages).

Mobile Application Interstitial Ad - is a full-screen advertisement, which may be placed as a “bumper” screen for the launch and exit of the application, or as a splash or jump page within the application. It may be used as the landing page from an earlier ad banner or may be a stand-alone Interstitial. This Interstitial may also be active or static.

Rich Media Mobile Ad (RMMA) - is a supplemental ad unit enjoying increased uptake in the Mobile Applications. Common to most RMMA ads is the two-stage principle of display and activation, whereby display is the way an RMMA ad resides in a usual ad space of a host property (application or website) and calls for action in form of a banner or similar. Only when the user interacts with the displayed banner by clicking on it or moving mouse-over do the RMMA features become activated showcasing their characteristic “rich” behavior. Respective guidelines are in advanced stages of development and expected to be added in future releases of this document. Draft RMMA Guidelines are available here: <http://www.mmaglobal.com/rmma.pdf>

- **Integrated Ad** – is an advertisement that is integrated with the application or game experience and is formatted to be compatible with the main content type used in the application context. It can be resized, reshaped and freely positioned as part of the core application content. Respective guidelines are under study and expected to be added in future releases of this document.
- **Branded Mobile Application** – many advertisers have looked at creating their own branded applications and uploading these into app stores. These take many different forms depending on the brand and its attributes. They can be entertaining, informative or functional. Illustrative examples include a Duracell running game, and a Nestle recipe app. Respective guidelines are under study and expected to be added in future releases of this document.
- **Sponsored Mobile Application** – is a publisher's downloadable application which features a sponsoring arrangement at various places across the application. (For example Nike or Adidas sponsoring a football app) Respective guidelines are under study and expected to be added in future releases of this document.

6.2 Mobile Application Advertising Unit Specifications

Specification Components

The following ad unit specifications provide the framework for producing In-App Display Ad creative material suitable across a broad range of mobile phones with a compelling and engaging user experience.

6.2.1 Media Formats The recommended formats for In-App Display Ads are:

- JPG, PNG or GIF as universal formats for still images.

- GIF for animated images.

6.2.2 Aspect Ratios The recommended aspect ratios for In-App Display Ads include:

- Mobile Application Banner Ads: See Table 1
- Mobile Application Interstitial Ad: Any landscape aspect ratio as per respective MMS Rectangle Ad unit. This typically includes 16:9 and 4:3 ratios and also a 1:1 (square) ratio. Portrait ratios are increasingly in common on modern smartphones in the 320 pixel width range.

6.2.3 Dimensions For graphical In-App Ad elements below 300 px or less width, widths and heights are recommended as defined for the respective Mobile Web Banner Ad units in Section 2.2 (except for the Text Tagline unit which does not apply in Mobile Applications), i.e.

- X-Large Mobile Application Image (width 300 pixels)
- Large Mobile Application Image (width 216 pixels)
- Medium Mobile Application Image (width 168 pixels)
- Small Mobile Application Image (width 120 pixels)

For graphical In-App Ad elements in the 320 pixel width range, the following best practice is arising

- XX-Large Mobile Application Image (width 320 pixels)
320 x 50
320 x 320
320 x 350
320 x 480

6.2.4 File Size File size considerations are currently ongoing for mobile applications. For the time being, following respective guidance from Mobile Web Banner and MMS Rectangle Ads is recommended (see Sections 2.2.4 and 4.2.4).

6.2.5 Display Length

Mobile Application Banner Ad units are displayed with application content

- Banner Ads may be replaced periodically with a new ad. Refresh intervals may vary by publisher and application.

Mobile Application Interstitial ads should be displayed in full, during which click-through actions are enabled.

- At any time the interstitial ad is displayed in full, the user should be able to click to continue past the ad into the content.
- A preliminary recommendation for interstitial ad display time is that the units disappear after a maximum of 5 seconds.

6.3 Mobile Application Advertising Creative Design Principles

6.3.1 Banner Ad Unit Creative Design Principles

Mobile Application Banner Ad units are presented alongside the host application. Banners may be presented anywhere on the screen at the publisher or developer's discretion.

Applications may contain a dividing area between the banner and application content, but this is application-specific and not considered a part of the ad unit specification. Banner ads are opaque (zero image transparency), such that the ad image does not blend with the application content.

Mobile Application Interstitial Ad units are intended for display on a complete screen or with minimal components of the application (e.g., title bar or soft-button labels). Generally, Mobile Application Interstitial ads should use as much of the screen area as possible. However, landscape or square aspect ratios seem to

allow the most flexibility across Mobile Application platforms, are convenient for advertisers, and leave room for the title bar and/or soft-button labels.

6.3.2 In-App Display Ad Unit Actions

In-App Display Advertising Units can either be:

- Non-active/non-highlighted/static means that the ad unit is visible on screen, but it is not clickable.
- Active/highlighted/non-static means that the ad unit is in the “select” state. Users can click on it for more information.

Action initiation:

Clicking on ad units provide opportunities for the user to receive additional information from the advertiser. Both ad banners and Interstitial ad images may be active and link either to places inside the application or to outside the application. This functionality must be consistent with a mobile phone’s capabilities (e.g., interactivity such as click-to-call, WAP push) and will be limited by both type of mobile phone and mobile phone connectivity. Examples include:

- **Click-to-Mobile Web:** click launches the web browser.
- **Click-to-call:** click initiates an outgoing call to the content provider or advertiser.
- **Click-to-video:** click initiates an advertiser’s video commercial for a product or service.
- **Click-to-SMS:** click initiates an SMS for a user to send a keyword to a shortcode to request more information.
- **Click-to-locate:** click initiates a map enabled by location-based services where a user may find, for example, the closest car dealer or movie theatre.
- **Click-to-buy:** click initiates a jump page where a user may make a purchase using some form of mobile payment (i.e. credit card, operator bill, etc).
- **Click-to-storyboard:** click transitions to a second interstitial ad (which itself may provide additional actions).

For applications and games whose flow may be greatly disrupted by a click-through, click-through ads should only display before the launch or exit of the application, or be queued until the end of the application experience, or avoided altogether. If it is required to switch the user away from the application context, the MMA recommends that, where possible, and in mobile phones that support click through, users are returned to the place in the application that they left after interacting with the ad (e.g., World Series of Poker, with \$1 million in chips).

If there is a risk that switching the user away from the application context will cause the application to terminate, requiring the user to completely re-launch of the application, the application developer or publisher is recommended to apply specific user warnings as follows:

- **Notification:** Clearly notifying users that they will be leaving the application environment to experience the advertisement. And clearly communicating that, in most cases, users will need to completely re-launch the application in the same way they started the application.
- **Right to Cancellation:** Giving users the option of interrupting the action to return to the application.

For ads displayed during the use of an application, MMA recommends using banners or interstitials that avoid switching the user away from the application context (e.g. expandable banners).

7.0 Technical Requirements for Mobile Advertisers

Advertiser/merchant site infrastructure

- Advertisers are responsible for the infrastructure costs for an advertising website or associated click-through pages including: keeping up with traffic demands, communications, hosting, hardware and software, as well as the costs of implementation.

Ad unit serving

- Ad-serving infrastructure will serve the ad units defined in these guidelines to phones, based on device-type detection and according to the best-fit principle, where the specification choice is based on what a particular mobile phone's screen can accommodate.
- Content that cannot be displayed by a mobile phone should not be delivered. For example, if a mobile phone does not support GIF, then that format must not be served to that particular mobile phone.

Ad format testing

- The MMA recommends that tests be conducted prior to launching a campaign.

Automatic resizing of ad formats (optional and where applicable)

- Ad-serving infrastructure may be capable of performing automatic resizing, where a standard dimension is dynamically adjusted to match the phone's display while maintaining the aspect ratio of the standard ad unit.
- Based on early experiences, automatic resizing works well for still images and provides value, such as the ability to support large screens. The absence of MMA guidelines should not stop companies from collecting experience in the field of automatic resizing by working along their own guidelines.
- Advertisers are advised to ensure that their creative is suitable for automatic resizing, especially in cases where visual detail is essential.

8.0 Who We Are

About the Mobile Marketing Association

The Mobile Marketing Association (MMA) is the premier global non-profit trade association established to lead the growth of mobile marketing and its associated technologies. The MMA is an action-oriented organization designed to clear obstacles to market development, establish mobile media guidelines and best practices for sustainable growth, and evangelize the use of the mobile channel. The more than 700 member companies, representing over forty countries around the globe, include all members of the mobile media ecosystem. The Mobile Marketing Association's global headquarters are located in the United States and it has regional chapters including North America (NA), Europe (EUR), Latin America (LATAM), Middle East and Africa (MEA) and Asia Pacific (APAC) branches. For more information, please visit www.mmaglobal.com.

About the MMA Mobile Advertising Committee

The MMA Mobile Advertising Committee, with active committee participation across the globe, has been established to create a library of format and policy guidelines for advertising within content on mobile phones. By creating mobile advertising guidelines, the MMA ensures that the industry is taking a proactive approach to keep user experience, content integrity and deployment simplicity as the driving forces behind all mobile advertising programs world-wide.



The MMA Mobile Advertising Committee is chaired by Madhouse, Inc., Verizon Wireless, Vodafone Group Services, Ltd. and Velti. This committee developed these guidelines in collaboration with the following MMA member companies:

MMA Global Mobile Advertising Committee - Global Members		
Alcatel-Lucent		mTLD Top Level Domain
Amdocs Inc.		Naqteq, a NOKIA Company
Camber Tech Inc.		OpenMarket
Catapult Marketing		Research in Motion
Comverse		Telecom Italia SpA
Ericsson AM		Telefonica S.A.
Google		The Hyperfactory
JumpTap		Turner Broadcasting System
Microsoft		Velti
MindShare		Vodafone Group Services
Mobtext		Yahoo!
Motricity		
MMA Global Mobile Advertising Committee – Regional Members		
<u>Asia Pacific</u>	<u>North America (cont.)</u>	<u>North America (cont.)</u>
Madhouse Inc.	Handmark Inc.	Rhythm NewMedia
<u>Europe</u>	Iconmobile, LLC	Ringleader Digital
Jinny Software	Impact Mobile Inc.	Smaato
Mobixell Networks Ltd	Isobar	TargetSpot
Orange NSM	MapQuest	Telescope, Inc.
Out There Media GmbH	Medialets Inc.	Texopoly
Turkcell İletişim Hizmetleri A.Ş	Mediamind	The Weather Channel Interactive
Unkasoft Advergaming	Millennial Media, Inc.	U.S. Cellular Corp
<u>North America</u>	Moclix	uLocate Communications Inc.
15 Miles	MobileCause	Vdopia, Inc.
4INFO, Inc.	Mobile Messenger	Verizon Wireless
Access Mobility/Cellepathic	Mobile Posse	Vibes Media
AT&T Mobility	Mocospace	Whoop Inc.
Cha Cha Search Inc	MSLGroup	Wireless Developer Agency
Collider Media	MySpace Inc. (Fox Interactive)	
Crisp Media	Myxer Inc.	
Fun Mobility	Nexage	
Greystripe Incorporated	Olive Media	

9.0 References

The following links provide additional sources of information and reference:

Guidelines and Best Practices

- MMA Global Code of Conduct
<http://www.mmaglobal.com/codeofconduct.pdf>
- MMA U.S. Consumer Best Practices Guidelines for Cross-Carrier Mobile Content Programs
<http://www.mmaglobal.com/bestpractices.pdf>

Educational Documents

- Mobile Applications
<http://www.mmaglobal.com/mobileapplications.pdf>

- Mobile Measurement Ad Currency Definitions
<http://www.mmaglobal.com/adcurrencies.pdf>
- Understanding Mobile Marketing: Technology and Reach
<http://www.mmaglobal.com/uploads/MMAMobileMarketing102.pdf>
- Off Portal – An Introduction to the Market Opportunity
<http://www.mmaglobal.com/offportal.pdf>
- Mobile Marketing Sweepstakes and Promotions Guide
<http://www.mmaglobal.com/mobilepromotions.pdf>
- Mobile Search Use Cases
<http://www.mmaglobal.com/mobilesearchusecases.pdf>
- Introduction to Mobile Coupons
<http://www.mmaglobal.com/mobilecoupons.pdf>
- Introduction to Mobile Search
<http://www.mmaglobal.com/mobilesearchintro.pdf>
- Short Code Primer
<http://www.mmaglobal.com/shortcodeprimer.pdf>
- Prevailing mobile in-application advertising formats (IAB study)
<http://www.iab.net/media/file/mobile-ad-formats-190710.pdf>

Websites

- Mobile Marketing Association Website
<http://www.mmaglobal.com>
- W3C Mobile Web Best Practices
<http://www.w3.org/TR/mobile-bp/>
- W3C mobileOK Basic 1.0 Guidelines
<http://www.w3.org/TR/mobileOK-basic10-tests/>
- W3C mobileOK Checker
<http://validator.w3.org/mobile>

10.0 MMA Guidelines Approval Process

The MMA implements a collaborative process for industry guidelines review and approval, prior to public release. The process not only considers feedback from industry leaders and experts but also helps to determine work streams for future releases. The summarized approval process is as follows:

- Committees generate a draft guidelines document developed and approved by MMA committee member companies (“Committee”).
- Once the guidelines are approved by Committee, the guidelines are issued for public review. Public review will last a minimum of four weeks.
- Feedback from the public comment period is circulated to Committee for review and incorporation as appropriate. Note: In the event substantial revisions are suggested, the Committee must again approve the guidelines prior to release.
- Once all approvals and feedback is gathered, incorporated and approved, the guidelines are released. The guidelines are released every six months and are the result of collaboration across the MMA Mobile Advertising Committee with representation from companies in Asia Pacific (APAC), Europe, Middle East and Africa (EMEA), Latin America (LATAM) and North America (NA). If deemed appropriate, the Committee may elect to release an interim revision of the guidelines.

11.0 Supporting Associations

The following associations currently support the MMA *Mobile Advertising Guidelines* in our collective mission to establish a consistent global guidelines and best practices for mobile advertising:

tbd

12.0 Contact Us

For more information, please contact:

Mobile Marketing Association

Email: mma@mmaglobal.com





www.mmaglobal.com

13.0 Glossary of Terms

The MMA maintains a nomenclature glossary of all terms within MMA guidelines, education documents and research. The glossary is available at:

<http://www.mmaglobal.com/glossary.pdf>.

Appendix 1 – WAP 1.0 Specifications

Appendix Table A-1: Technical Specifications – WAP 1.0 Banners		
Ad Unit	Technical Specifications	Sample Creative
Asia Pacific: Standard Text Link for 128 and 176 screen sizes	<ul style="list-style-type: none"> • 1 line of text maximum • Up to 8 characters maximum 	ABCD酷炫网站
Asia Pacific: Text Link for 240 screen size	<ul style="list-style-type: none"> • 1 line of text maximum • Up to 12 characters maximum 	ABCD广告片流畅下载
Europe, Middle East and Africa: Standard Text Banner	<ul style="list-style-type: none"> • 3 lines of text maximum • Up to 16 characters per line • Max. 35 characters total, including spaces 	
Europe, Middle East and Africa and North America: Standard Image Banner	<ul style="list-style-type: none"> • 80 x 15 pixels • B&W, 1-bit bitmap • < 200 bytes file size 	
Europe, Middle East and Africa and North America: Standard Image/Text Combination Banner	<ul style="list-style-type: none"> • 80 x 12 pixels • B&W, 1-bit bitmap • Text: Up to 16 characters • < 200 bytes files size 	
North America: Standard Text Banner	<ul style="list-style-type: none"> • 2 lines of text maximum • 12-16 characters per line • 32 characters total, including spaces 	

Aspect Ratios see Table A1 above.

Dimensions see Table A-1 above.

Media Formats The recommended formats for WAP 1.0 Banner Ads.

- bmp (1-bit bitmap)
- Text ads are based on the default mobile phone character format.

File Sizes see Table A-1 above.



NEW YORK • LONDON • SINGAPORE • SÃO PAULO

Mobile Application Privacy Policy Framework

December 2011

Final, After Public Comment Review

**Issued by the MMA Privacy & Advocacy
Committee**

December 2011

Introduction

The Mobile Marketing Association is the premier, global not-for-profit trade association that works to promote, educate, measure, guide and protect the mobile marketing industry worldwide. In this capacity, we are pleased to introduce the attached Mobile Application Privacy Policy, authored and prepared by the MMA Privacy & Advocacy Committee.

The intent of this privacy policy is to provide the mobile application developer with policy language that can be quickly and completely understood by the consumer.

Goal for the Privacy Policy

*The MMA Privacy & Advocacy Committee intends for this mobile application privacy policy to be used as a starting point for most mobile applications. The policy is designed to address the core privacy issues and data processes of many mobile applications, but should not be considered sufficient by itself to cover all types of applications. There are many areas where many in the mobile marketplace are experimenting with privacy enhancing technologies, and we applaud those efforts. The core goal for this privacy policy framework is to encourage the mobile application developer community to continue to move consumer privacy interests forward. **We strongly encourage those using this model policy to consult an attorney and/or privacy professional when crafting your own policy.***

Instructions for using this Privacy Policy

The policy that follows contains two kinds of annotated instructions. The first, *in blue italics*, provide the app developer specific advice on the use of the core principles contained herein. The second, **[IN BLUE CAPS, and within brackets]**, are sections that need to be uniquely tailored by the app developer to the specifics of their application and its use of consumer information. ***In all cases, the app developer should consult with legal counsel or privacy professionals to ensure that your policy and compliance procedures are in alignment.***

MMA Privacy & Advocacy Committee Member Companies

This committee is co-chaired by Alan Chapell, President of Chapell & Associates, and Fran Maier, President of TRUSTe, and the MMA is grateful to them for their leadership and commitment to all of our privacy initiatives.

3Cinteractive

4INFO, Inc.

Acxiom Corporation

Aegis Mobile, LLC

Air2Web

Alcatel-Lucent

AT&T AdWorks

Cellfish Media LLC.

CellTrust Corporation

Cha Cha Search, Inc.

Chapell & Associates

Collider Media, Inc.

comScore, Inc.

CTIA

Future Of Privacy Forum

g2

Handmark Inc.

Hogan Lovells US LLP

ImServices

Inmar

InMobi

JumpTap

Media Contacts

Medialets, Inc.

Millennial Media, Inc

Microsoft

Mobclix

Mobile Intelligence Solutions, Inc.

Mojiva, Inc

Motricity

MTV Networks

Neustar, Inc.

Nexage, Inc.

OpenMarket

Pontiflex

Poynt Corporation

Predicto Mobile LLC

PreEmptive Solution

Procter & Gamble

Safecount

Smiley Networks, Inc.

Sprint-Nextel

Syniverse Technologies

The Nielsen Company

TRUSTe

Turner Broadcasting System, Inc.

Unilever

Velti

Verizon Wireless

Vibes Media

WHERE, Inc.

Yahoo!

Mobile Application Privacy Policy (Annotations for guidance) 15Dec2011

*The MMA Privacy & Advocacy Committee intends for this mobile application privacy policy to be used as a starting point for most mobile applications. The policy is designed to address the core privacy issues and data processes of many mobile applications, but should not be considered sufficient by itself to cover all types of applications. **We strongly encourage those using this model policy to consult an attorney and/or privacy professional when crafting your own policy.***

This privacy policy governs your use of a software application (“Application”) on a mobile device that was created by [APPLICATION DEVELOPER NAME.] The Application includes [BASIC DESCRIPTION OF APP features, functionality and content such as: games, news, messages, and more.]

What information does the Application obtain and how is it used?

This section is designed to inform Users of the types of data that the app obtains and how that information is used. While we’ve provided several types of data that are often obtained by apps, the App Developer should make a reasonable attempt to ensure to provide Users with a clear, illustrative list of the most important data points obtained by each app. Moreover, the model policy attempts to draw a distinction between data that is provided directly by a User (“User Provided Information”) and data that is collected automatically by the Application (“Automatically Collected Information”). The MMA recognizes that this distinction may not be in harmony with the data privacy practices of all Applications, and therefore encourages App Developers to work to an attorney and/or privacy professional to ensure that the information they provide in this section is in line with the actual data flows for each Application(s).

User Provided Information – The Application obtains the information you provide when you download and register the Application. [IF APPLICABLE] Registration with us is optional. However, please keep in mind that you may not be able to use some of the features offered by the Application unless you register with us.

[IF APPLICABLE] Registration with us is mandatory in order to be able to use the basic features of the Application.

Mobile application developers should be aware that certain types of data, for example, medical records and certain types of financial information may be subject to existing privacy law. Application developers creating apps that collect potentially sensitive information are

encouraged to obtain counsel to ensure that their data collection policies are in line with current law in the jurisdiction(s) where the app may be used.

When you register with us and use the Application, you generally provide [INSERT A REPRESENTATIVE LIST HERE – A FEW TYPICAL EXAMPLES ARE PROVIDED FOR REFERENCE]: (a) your name, email address, age, user name, password and other registration information; (b) transaction-related information, such as when you make purchases, respond to any offers, or download or use applications from us; (c) information you provide us when you contact us for help; (d) credit card information for purchase and use of the Application, and; (e) information you enter into our system when using the Application, such as contact information and project management information. We may also use the information you provided us to contact you from time to time to provide you with important information, required notices and marketing promotions.

If the Application collects information from and/or for social networking platforms (e.g., pulling contact information, friends lists, login information, photos or check-ins) the Application should ensure that the prior consent of the user is obtained.

Automatically Collected Information - In addition, the Application may collect certain information automatically, such as [INSERT A REPRESENTATIVE LIST HERE – a few typical examples are provided for your reference] the type of mobile device you use, your mobile device's unique device ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browsers you use, and information about the way you use the Application. See "Automatic Data Collection and Advertising" section for examples.

Does the Application collect precise real time location information of the device?

This section is only applicable if the Application collects precise, real-time location information. Non-precise location information such as geo-targeting (e.g., zip code or city) data is typically addressed elsewhere in the privacy policy (e.g., the section entitled "automatic data collection and advertising.")

[IF No] This Application does not collect precise information about the location of your mobile device.

[IF Yes] This application does collect precise information about the location of your device. [INSERT A GENERAL DESCRIPTION OF HOW THIS IS DONE IN A WAY THAT IS CLEAR TO AN AVERAGE CONSUMER.]

We use your location information to Provide requested location services, and [INSERT A LIST OF OTHER USES (E.G., TO ALLOW TAGGING, OR TO CHECK-IN) AND IF APPLICABLE, DESCRIBE THE CIRCUMSTANCES WHERE PRECISE LOCATION DATA IS SHARED WITH THIRD PARTIES FOR THEIR INDEPENDENT USE.]

[IF APPLICABLE] You may at any time opt-out from further allowing us to have access to your location data by [state how user can manage their location preferences either from the app or device level]. For more information, please see the section below entitled “opt-out rights.”

Do third parties see and/or have access to information obtained by the Application?

Generally, app developers will want to have the right to transfer information collected by the app under certain circumstances. For example, if the app developer sells the app, the developer may want that information collected by the application transferred as part of the sale. While we’ve provided some of the more common examples of data transfer to third parties, app developers are encouraged to work with counsel and/or privacy professional to determine if other examples should be included in their policy.

Yes. We will share your information with third parties only in the ways that are described in this privacy statement.

We may disclose User Provided and Automatically Collected Information:

- as required by law, such as to comply with a subpoena, or similar legal process;
- when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request;
- with our trusted services providers who work on our behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth in this privacy statement.
- if [APP COMPANY NAME] is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our Web site of any change in ownership or uses of this information, as well as any choices you may have regarding this information;

- **[IF APPLICABLE]** to advertisers and third party advertising networks and analytics companies as described below under the Section entitled Automatic Data Collection and Advertising.

Automatic Data Collection and Advertising

Mobile application developers should be aware of which mobile advertising networks and other third parties they are working with in order to determine if that ad network or other third party is offering an opt-out. At a minimum, application developers should take into account whether the app is advertising supported and whether data is obtained by an ad network or other third party for the purpose of ad targeting.

[IF APPLICABLE] This Application is supported via advertising, and collects data to help the Application serve ads. **[IF APPLICABLE]** We may work with analytics companies to help us understand how the Application is being used, such as the frequency and duration of usage. **[IF APPLICABLE]** We work with advertisers and third party advertising networks, who need to know how you interact with advertising provided in the Application which helps us keep the cost of the Application low **[or free]**. Advertisers and advertising networks use some of the information collected by the Application, including **[IF APPLICABLE]** the unique identification ID of your mobile device and **[IF APPLICABLE]** your mobile telephone number. To protect the anonymity of this information, we use **[IF APPLICABLE]** an encryption technology to help ensure that these third parties can't identify you personally. These third parties may also obtain information about other applications you've downloaded to your mobile device, the mobile websites you visit, your non-precise location information (e.g., your zip code), and other non-precise location information in order to help analyze and serve anonymous targeted advertising on the Application and elsewhere. **[IF APPLICABLE]** We may also share encrypted versions of information you have provided in order to enable our partners to append other available information about you for analysis or advertising related use.

If you'd like to opt-out from third party use of this type of information to help serve targeted advertising, please visit the section entitled "Opt-out" below.

What are my opt-out rights?

Mobile application developers should be aware of which mobile advertising networks and other third parties they are working with in order to determine if that ad network or other third party is offering an opt-out. We recognize that the mobile marketplace continues to experiment with different types of opt-out mechanisms – and strongly encourage the mobile application developer community to participate in these experiments to the benefit of consumer privacy interests.

There are multiple opt-out options for users of this Application:

Opt-out of all information collection by uninstalling the Application – You can stop all collection of information by the Application easily by uninstalling the Application. You may use the standard uninstall processes as may be available as part of your mobile device or via the mobile application marketplace or network.

[IF APPLICABLE] Opt-out from the use of information to serve targeted advertising by advertisers and/or third party network advertisers

[IF APPLICABLE] You may at any time opt-out from further allowing us to have access to your location data by [state how user can manage their location preferences either from the app or device level].

Data Retention Policy, Managing Your Information

We will retain User Provided data for as long as you use the Application and for a reasonable time thereafter. If you'd like us to delete User Provided Data that you have provided via the Application, please contact us at privacy@XXXXXX.com and we will respond in a reasonable time. Please note that some or all of the User Provided Data may be required in order for the Application to function properly, and we may be required to retain certain information by law.

Children

Mobile application developers should be aware of and ensure that the app and the app developer's privacy practices are in compliance with the Children's Online Privacy Protection Act (COPPA). Developers should pay particular attention to COPPA when creating apps that contain cartoon characters or other features that may cause the app to be perceived as being directed towards children under 13. Application developers creating apps that might be governed under COPPA or similar laws are encouraged to obtain counsel to ensure that their data collection policies are in line with current law in the jurisdiction(s) where the app may be used.

We do not use the Application to knowingly solicit data from or market to children under the age of 13. If a parent or guardian becomes aware that his or her child has provided us with information without their consent, he or she should contact us at privacy@XXXXXX.com. We will delete such information from our files within a reasonable time.

Security

Application developers should ensure that their security procedures are reasonable, and should provide an overview of their security procedures below.

We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees and contractors who need to know that information in order to operate, develop or improve our Application. Please be aware that, although we endeavor to provide reasonable security for information we process and maintain, no security system can prevent all potential security breaches.

Changes

Application Developers should be aware that retroactive, material changes to privacy practices generally require the prior consent of the User.

This Privacy Policy may be updated from time to time for any reason. We will notify you of any changes to our Privacy Policy by posting the new Privacy Policy here [INSERT URL] and [AS APPLICABLE, IF THE APPLICATION OBTAINS EMAIL AND/OR PHONE #] informing you via email or text message. You are advised to consult this Privacy Policy regularly for any changes.

Your Consent

By using the Services, you are consenting to our processing of User Provided and Automatically Collection information as set forth in this Privacy Policy now and as amended by us. "Processing," means using cookies on a computer/hand held device or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information, all of which activities will take place in the United States. If you reside outside the U.S. your information will be transferred to the U.S., and processed and stored there under U.S. privacy standards. By using the Application and providing information to us, you consent to such transfer to, and processing in, the US.

Contact us – If you have any questions regarding privacy while using the Application, or have questions about our practices, please contact us via email at Privacy@XXXXXX.com.

FILED/ACCEPTED

JUN 29 2011

Federal Communications Commission
Office of the Secretary

“Wrap Up on Privacy and Location Based Services”

Professor Peter Swire

Ohio State University

Federal Communications Commission:

“Helping Consumers Harness the Potential
of Location Based Services”

June 28, 2011

Overview

- Outside DC: “The sense of excitement and wonder” about LBS
- But, privacy risks
- When to publish or withhold “presence” (Griffin)
 - Notice/transparency
 - Choice and meaningful choice
- Getting to some new best practices
 - What will be obvious five years from now, and how can we get there sooner?

“Sense of Excitement & Wonder”

- Tim S.: today consumers get real advantages from publishing their location
- Coupons: from the Sunday grocery store circular to a basic tool of my law students' lives – maybe you can pay your monthly phone bill with these discounts
- More gifts: from flowers on Mother's Day to BuyYourFriendDrink
- Serendipity:
 - You find your old friend
 - You don't miss seeing your old friend – fewer trains pass in the night
- Game dynamic – life is more fun
- Carriers – a platform to make your device better
- Many other advantages
 - Fraud prevention, public safety (CPR)
 - Dense mobile ecosystem, innovation, and economic growth

Privacy Risks

- Privacy experts spot risks associated with location information
 - One-time shift to a world where we carry location tracking devices
- Government sees all:
 - Surveillance of civil society
 - Location relevant to proving a large fraction of criminal cases
 - Supreme Court case next term on GPS tracking & Leahy bill
- Marketers see all:
 - Current debates about targeted marketing & price discrimination
 - Blaze: “Mobile aps are currently typically written by service providers, which want to collect as much user data as they can”
- Others see all:
 - Burglars know I’m not home, stalkers can find my kid, and teenagers might not want parents to track them
- Which of these risks are realistic in practice?

Publish or Withhold “Presence”

- Familiar principles of notice & choice at center of policy discussion
- Notice: some background
 - Future of Privacy Forum: 22 of 30 top paid aps no privacy policy
 - Brookman/CDT: most top aps gather geolocation
 - Similar history for web sites around 1997 of no policies
- Notice: good practices
 - Panelists agree should have good privacy policies for geolocation
 - Limited real estate on mobile devices
 - Usability on small screen
 - Just in time notice
 - Build “smarts” into notices, to comply with user preferences
 - Hard to be consistent across aps/devices/OS
 - Evolve toward standard notices – financial privacy example

Choice about “Presence”

- Broad acceptance of opt-in to collect geolocation information for apps
 - The basic choice – consumer chooses the app/device or doesn't
 - Some services have multiple opt-ins, stricter than in many other sectors
- Some issues of “meaningful choice”
 - Active choice vs. passive collection
 - “Glimpse” vs. a service turned on once and then continues
 - Gather data only for a defined purpose vs. a bundled service (you use the service, we collect and perhaps sell all that data)

Moving Toward New Best Practices

- Rapid change and innovation (8000x increase in ATT mobile data traffic in 3 years)
- Optimism from some recent rounds of innovation:
 - 1990s web privacy policies: 12% to 88% in three years
 - Software downloads – uninstall as standard feature
 - EULAs – can save and print now
 - Spam, but CAN-SPAM and easy to opt out now from legitimate companies

Moving Toward Best Practices

- A problem: limited compliance staff in the garage
 - Over time, big fraction of Internet traffic in major players with privacy compliance; pattern may repeat for mobile aps
 - Long tail exists of smaller players
 - But privacy risks highest in big databases, where compliance staff does exist
 - Trustmarks can help with smaller players
- Length of time to retain data
 - Search engines and “every search you ever made”
 - Now, major search engines anonymize after a number of months
 - Location information and “every place you have ever been”
 - Many of the services (coupons, location of your friend) are for today’s location
 - Privacy risks reduced a lot if limit time that location is kept in identifiable form

Concluding Thoughts

- Two things to watch
 - A risk that consumers can't turn on/off for location information that is widely shared
 - The eco-system must learn to work together to treat location data as sensitive
- Lots of reason for optimism
 - Sense of wonder, excitement, and growth
 - Consumers will learn to manage how to publish or withhold "presence" – Boyd research on how they do that already on social networks
 - Emerging major players will develop privacy practices
 - Government can play a role for now in increasing transparency and encouraging best practices

Location-Aware Mobile Applications: Privacy Concerns & Best Practices

By Janet Jaiswal, Director, Enterprise BU TRUSTe and Saira Nayak, TRUSTe consultant

Location-Aware Apps – What’s All the Fuss About?

Companies of all types are deploying innovative mobile applications featuring “geo-location,” a technology that uses data obtained from an individual’s mobile device¹ to identify or describe their actual physical location at a given point in time. Location-aware applications or “apps” are already becoming a ubiquitous feature of the mobile web thanks to widespread adoption of GPS-enabled Smartphones such as the iPhone, Droid etc. which are owned by more than 42 percent of US citizens as of Dec 2009².

Already, companies are recognizing the benefits of “geo-marketing.” Location-aware apps bring discounts and promotions directly to user at the point of purchase and provide valuable, real-time data about customer preferences. This data can be used, in aggregate, to provide data on key market trends, or integrated into a customer profile to provide a more personalized experience. It would be difficult to compile this type of information through a more efficient process using any other currently known technology. Consumers benefit too - from access to information that can be instantly relevant to a purchasing decision, to location-specific discounts and services.

As the rise in the use of location-aware apps and geo-marketing continue, concerns keep on growing around online privacy – specifically, business practices around the collection and use the personal identifiable (PII) data. The risk of identity theft increases with each collection of PII, especially when the information is not maintained securely. In addition, a combination of data elements – even elements that are not individually PII – can be used to personally identify an individual. Technology that can match PII with a user’s location presents an additional layer of privacy concern. Regulators are aware of such concerns and are moving swiftly to enact rules around how companies can use geo-location data, especially in marketing to younger users. In this climate, companies should think carefully about their geo-marketing practices and examine whether their current privacy policies accurately reflect the collection and use of geo-location data.

According to a survey of more than 4,000 mobile device users conducted by KPMG³, more than 87 percent have concerns about both privacy and security on their mobile device. The same survey shows that more than 66 percent of U.S. consumers are not comfortable using their mobile phones for financial transactions. Another survey conducted by Webroot⁴ shows that more than 55 percent of Smartphone users fear loss of privacy through mobile applications with geo-location services.

1. “Mobile Device” is a portable electronic device which allows the user to process, receive, and send data through a common carrier without being limited to a specific geographical location.

2. January 4, 2010 survey by ChangeWave Research Survey

3. KPMG Mobile Banking Survey 2009 of 4,190 mobile device users.

4. Geolocation Survey conducted by Webroot on July 13, 2010

This white paper delves into some of the policy concerns and market dynamics around location-aware apps. We also provide you with some best practices that can help you minimize the privacy and data security risks that may arise when deploying location-aware apps.



Location-aware Apps: A Market Overview

Geo-location technology, in use since 1999, has a wide range of applications from automated payment processing to electronic tolling. On your phone, location apps work to identify your current location using your computer's IP address or your Smart phone's GPS chip.

This year will probably be remembered as the year that geo-location went mainstream as many companies, including Internet giants Facebook, Twitter and Google launched products and services that brought the benefits of geo-location to their users. With Twitter Places, which was launched in tandem with the 2010 World Cup, users can tag their tweets with specific places. Facebook Places allows users to "check" themselves and their friends in at locations such as restaurants, bars, parks and other places of interest. It also allows Facebook friends to help users discover content or available products. Google Places launched in April 2010 builds on prior Google business listings and offers up Web pages dedicated to individual businesses, showing where they are located, provides street-level images, and customer reviews of services or products.

Location-aware apps can also be plugged into existing social media platforms allowing third-party developers to integrate geo-location apps into their service. This means that with little technological investment, a company can leverage the capabilities of existing platform services - like Facebook - to further its marketing strategy by allowing them to supply local information and advertising. For example, Booyah, a "location-based video-game company," is the creator of myTown, one of the most popular iPhone apps. The company recently launched InCrowd, a location-aware app built on Facebook Places technology, which lets users interact with friends and share posts in real-time in real-world locations.

Several fast growing online companies have built their business around geo-location services. These include Loopt, whose mobile app allows you to check-in to various locations (retailers, restaurants), and instantly share your check-ins with your network. Loopt also works with retailers to provide coupon offers at the point of interest, eliminating the need to coupon clip. Another popular location-aware service is Foursquare, which combines the fun of a game with the utility of geo-location by allowing you to earn badges based on the number of places you've checked into. The company recently introduced a tool that allows participating businesses to see data on their Foursquare-using customers: number of check-ins, how many check-ins are male or female, etc. Lastly, Gowalla, like Foursquare, allows users to check into places in order to collect digital goodies and is focusing on smaller cities than Foursquare.

Retailers are also integrating geo-location into their marketing efforts. For instance, The North Face and Sonic Drive-In are leveraging geo-fencing capabilities with ShopAlert that will enhance a customer's brick-and-mortar shopping experience by providing a personal marketing message to a consumer entering or exiting the defined area that is presumably near a retail location. The ShopAlert program "lets a company customize the offer by location, time of day, and available offer," said Alistair Goodman, CEO of Placecast, creator of ShopAlerts. Furthermore, Pepsi is about to launch Pepsi Loot, which it describes as "the first geo-based iPhone application that has a loyalty program associated with it." This location app will connect users to the ecosystem of over 200,000 restaurants or "Pop Spots" that serve Pepsi products. With its many locations, Pepsi customers will have plenty of opportunities to earn and redeem Loot points for discounts and other goodies (like exclusive music and video downloads). Pepsi is also working to integrate its loyalty program into Foursquare's mobile app where Pepsi Loot users would get a Foursquare notification when they are close to a Pepsi Pop Spot.

These examples illustrate the rich diversity of companies (and business models) currently integrating geo-location into their product or market strategy.

Privacy and Safety Concerns with Location-Aware Apps & Services

Despite the promising benefits of geo-location technology, many users have significant privacy concerns around its use, particularly in location-aware mobile devices. This was demonstrated most recently in a study by researchers at Carnegie-Mellon⁵, whose research identified the following areas of user concern:

- Who is collecting location data, how it is used, with whom it can be shared with and how long it can be stored.
- Being spammed by advertisements or offers based on their physical location.
- Accidental or unintentional sharing of location data resulting in annoyance, embarrassment or danger to an individual's safety.

5. Location-Sharing Technologies: Privacy Risks and Controls by Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, Carnegie Mellon University, Updated February 2010

These findings reflect a growing consensus that geo-location data should be classified as sensitive due to a number of concerns such as transparency about a company's data collection practices, solicitations made based on geo-location data obtained without the user's consent, and physical safety stemming from the misuse of information that can identify a user's current or future physical location.

Companies engaging in geo-marketing should be aware of the sensitivity of geo-location data when implementing business practices and corresponding privacy policies. Clearly, combining geo-location data with detailed user profile information for targeted marketing efforts can significantly increase a company's privacy risk, especially when the user has not specifically agreed to the practice. We've already seen how user concern over personal information collection and use by a product or service can lead to that product or service's downfall such as with Facebook's ill-fated Beacon advertising program which has since been removed. These concerns would be multiplied significantly if the unauthorized PII collection included geo-location data.

The physical safety concern is particularly important since geo-location data can become dangerous information in the wrong hands. Stalkers or thieves with knowledge of an individual's present or future location can use this data to directly harm individuals and/or their property. In a project meant to underscore the potential harm posed by freely shared location information, a group of consumer advocates created a website - www.pleaserobme.com - that aggregated public Twitter users' location information. The project gained considerable press coverage - not just because it raised the possibility of physical safety, but also privacy. Most individuals don't want their co-workers, neighbors or even family to know where they are at any given point in time. In some cases, the revelation of this information could lead to embarrassment or even the loss of a job or a relationship.

Companies should also pay attention to the Carnegie-Mellon findings related to user concern about spam. Knowing someone's location allows you to push contextually-relevant information to them such as info about their nearby friends, advertisements for local businesses, sightseeing recommendations etc. However, identifying what is relevant can be a challenge, especially when geo-marketing is used in excess, resulting in information overload. Consumers that view a location-aware mobile technology as "spammy" will simply tune out or drop use of that product or service altogether.

The future of geo-location technology and location-aware apps is closely aligned with the ongoing debate around what constitutes effective regulation of privacy and data security online. Congress is currently considering federal privacy legislation that will impose additional notice obligations on companies with regards to the collection and use of personal data. This legislation would classify geo-location data as sensitive and would require a user opt-in to use of this type of data for online advertising or marketing purposes. Laws around geo-location are even stricter in other countries; Europe's e-privacy Directive for instance, states that an individual's location data⁶ may not be stored once the service is provided unless the data is needed for billing and interconnection purposes⁷.

6. Source: Discussion draft of the yet un-named legislation on May 4, 2010. http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf

7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Article 9, paragraph 1, OJ L 201, 31.1.2002.

Even in the absence of a national privacy law here in the US, the FTC has signaled its intent to articulate a privacy rules framework to protect consumers' privacy online, while also supporting self-regulatory approaches. The FTC began laying the groundwork for some of these rules in its ongoing review of behavioral advertising, which it defines as "the tracking of consumers" online activities over time...in order to deliver advertising targeted to the individual consumer's interests. Their review culminated in the agency's FTC's Self-Regulatory Principles for Behavioral Advertising.⁸ While the Principles are not binding rules, they do provide guidance for self-regulatory efforts. Principle 4 specifically requires that companies get "affirmative express consent" when using sensitive data; furthermore, the Report classifies geo-location data as sensitive. This means that companies should strongly consider using opt-in notice for location apps - especially if the intended use is for targeted advertising or marketing efforts.

Companies that market online products and services to individuals under the age of 13 should also be aware of the FTC's ongoing review of the Children's Online Privacy Protection Act ("COPPA"). The FTC is aware of the growing rate of Smartphone adoption among younger users; it is also aware of the public safety concerns posed by geo-location technology. The agency just closed its comment review on COPPA and is considering, among other things, whether to expand the definition of "personal information" under the rule to include "mobile geo-location data."⁹

Consumer advocates have also been publicly vocal about their policy concerns with geo-location technology. These concerns mostly focus on the ability of governments and other entities to create comprehensive data profiles that may compromise a user's locational and other privacy. The Electronic Frontier Foundation, in its whitepaper¹⁰ on locational privacy, highlights two additional concerns: retention of geo-location data may subject a company to legal requests for data, and storing geo-location data over extended periods of time will increase the likelihood of identity theft.

Addressing the Privacy Concern: Know Your App & Mobile Web Site

Even with the changing regulatory climate around online privacy, there are some simple steps that companies can take to minimize the privacy and data security risk from the launch of a location-aware app.

8. FTC BA Principles Report, <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>

9. See, FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule, <http://www.ftc.gov/opa/2010/03/coppa.shtm>

10. On Locational Privacy And How to Avoid Losing it Forever, <http://www.eff.org/wp/locational-privacy> by Andrew J. Blumberg & Peter Eckersley, Electronic Frontier Foundation

Perform Factual Due-Diligence

Knowing what your location-aware app does, what type of data it collects, and whether that data is shared with affiliates, partners or third parties, is an important first step in determining which best practices are needed to address the privacy and security concerns posed by geo-location data. When developing a location-aware app, companies should review their existing information security practices to determine what type of personal information is already being collected and the data flows for that information. They should examine the data being collected. For example, is the data personally identifiable, either individually or when combined with other elements in a company's database? Then the company will need to look closely at the data flows from its location-aware offering. Will it share this data with an online advertiser or marketer? Will the company host the location app on its own mobile or internet website, or on a social-media platform like Facebook? Or, does the company want to develop a virtual loyalty-based program for its users using geo-location platform services like Loopt or Foursquare? These important questions should be part of a company's factual due diligence process when determining the best practices and policies around location-aware apps.

Review Partner & Platform Policies

It's always a good idea to review the terms of service and privacy policies of other parties implicated by the launch of your location-aware app or service. For instance, companies developing location-aware apps for the BlackBerry computers will want to review RIM's AppWorld developer agreement to make sure that their policies are consistent with RIM's requirements. Similarly, companies working together on the launch of a location-aware app should review each other's data privacy and governance policies - especially if sharing geo-location data is part of the agreement.

Get a Little Creative

With the proliferation of location apps on Smartphones, companies may need to start thinking about different, more creative forms of notice¹¹ to comply with federal or state laws - or risk losing users who eventually tire of being notified every single time the app is opened. Take the example of a mobile store locator app - a notification each time you open the app to locate a store would be redundant, especially since you are electing to have the app guide you to the store's location in the first place. A less intrusive method that would be just as effective, could be an initial notification - supplemented by key reminders for important events like software updates.

¹¹ It is notable that the following language was added to the final version of the FTC Behavioral Advertising Report: "Where the data collection occurs outside the traditional website context, companies should develop alternative methods of disclosure and consumer choice that meet the standards described above (i.e., clear, prominent, easy-to-use, etc.)." FTC BA Principles Report, at 48.



Be Mindful of Existing Privacy & Security Laws

Companies should be mindful of existing obligations under federal and state laws for collection and protection of personal information. These include:

FTC Act – specifically §5 which prohibits unfair and deceptive trade practices.

Children's Online Privacy Protection Rule – governs the online collection of personal information from children and applies to websites and online services that are directed to children under the age of 13.¹²

FTC Behavioral Advertising Guidelines

HIPAA & FTC Health Breach Rule - for location-aware apps developed by “covered entities” and their “business associates under HIPAA.¹³

FACT & The FTC Red Flag Rules – which require that “creditors” and “financial institutions” develop written information security programs that identify potential “red flags” for identity theft.¹⁴ Companies that come within the ambit of this rule may consider red-flagging geo-location data - particularly if it is used in combination with personal information to deliver targeted ads or services.

Section 222 of the Federal Communications Act – requires that telecommunications providers take specific steps to secure customer proprietary network information (CPNI).¹⁵

Electronic Communications Privacy Act - sets out requirements under which the government can access private Internet communications. This includes elevated process such as a warrant for certain categories of personal information that are considered “content.”¹⁶

State Security breach notification laws – a majority of states have laws that require consumers be notified in the event that their “personal information” is “breached.”¹⁷

12. 16 C.F.R. §312

13. 42 CFR Part 2. §164.501

14. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 681 (2007)

15. CPNI data includes phone numbers called, frequency, duration and timing of such calls and related services purchased by the consumer. 47 U.S.C. §151 (1996)

16. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510

17. E.g. FLA. STAT. ANN. §817.5681 (1)(a) (2009). According to a recent post on the Proskauer privacy blog, 46 states – with the exception of Alabama, Kentucky, New Mexico and South Dakota – now have data breach laws. <http://privacylaw.proskauer.com/2010/04/articles/data-breaches/its-not-too-late-to-come-to-the-party-mississippi-joins-45-other-states-by-enacting-a-security-breach-notification-law/>

18. California enacted the nation's first general information safeguard law. CAL. CIV. CODE §1798.81.5(b) (2009)

State Safeguard Laws - eight states, including California, Maryland and Texas – have enacted general safeguard laws to protect personal information.¹⁸

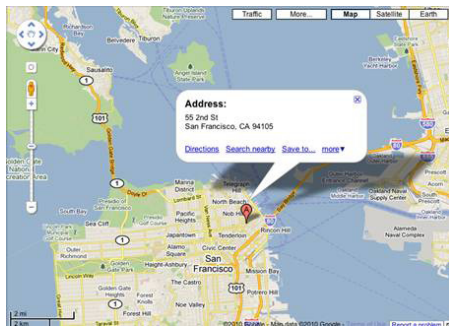
State Business Record Disposal laws - over 19 states now have laws that regulate the disposal of business records containing personal information.¹⁹

Massachusetts Data Security Regulations – obliges companies to encrypt the personal information of Massachusetts’ residents.²⁰ These encryption requirements apply broadly and include personal information stored on laptops as well as other portable devices.²¹

Applicable Law from other Jurisdictions - companies should consult laws and guidance from other, relevant jurisdictions when deploying a location-aware app.

Ensure that Notice Matches Up to Practice

Before a location-aware app is publicly launched, the company should amend its information security practices, as well as its privacy and other notices, to reflect the additional collection and use of geo-location data. It’s important to remember that under Section 5 of the FTC Act and similar state statutes such as the Massachusetts Consumer Protection Act, companies can be prosecuted for privacy violations stemming from a “deceptive” notice”. Put differently, a company that captures data for one purpose and then proceeds to use that same data for another purpose that is inconsistent with its privacy policy, may be liable under state and federal²² deceptive trade practices laws. To avoid this type of risk, companies should make sure that their data collection and use matches what is laid out in the company’s privacy policies and notices. A company can also be found to have engaged in an “unfair” practice, under federal²³ and state²⁴ laws, for failing to protect personally identifiable data.



19. E.g., CAL. CIV. CODE §1798.81 (2009)

20. Standard for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00 (2009), <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

21. 201 CMR 17.04(5)

22. 201 CMR 17.04(5)

23. 15 U.S.C. § 45 (a)(1). See e.g. In the Matter of Life is good, Inc., FTC Docket No. C-4218 (Apr. 16, 2008) (alleging that the company violated promises about the security provided for customer data); In the Matter of Petco Animal Supplies, Inc., FTC Docket No.C-4133 (Mar. 4, 2005) (same)

24. See CAL. BUS. & PROF. CODE, §17200 (West, 2009)

How Can TRUSTe Help?

TRUSTe has certified thousands of companies in the area of online privacy since 1997. TRUSTe's new mobile privacy certification program redefines privacy for mobile internet usage, giving businesses the ability to quickly reassure mobile customers that they can trust the applications with their personal information especially geo-location information. The certification for privacy involves a thorough review of each mobile application or mobile website to ensure adherence to privacy standards, as well as laws, regulations, best practices and emerging standards such as the ones highlighted earlier.

The TRUSTe mobile privacy certification program helps companies successfully use technologies such as geo-location, social networking technologies such as Facebook's Places and more for their mobile applications and mobile web sites – leading to more conversions on that platform.

To learn more go to www.truste.com/mobile

Learn More

Contact TRUSTe at 415.520.3490 or visit www.truste.com/mobile to learn more about TRUSTe's Mobile Privacy certification.