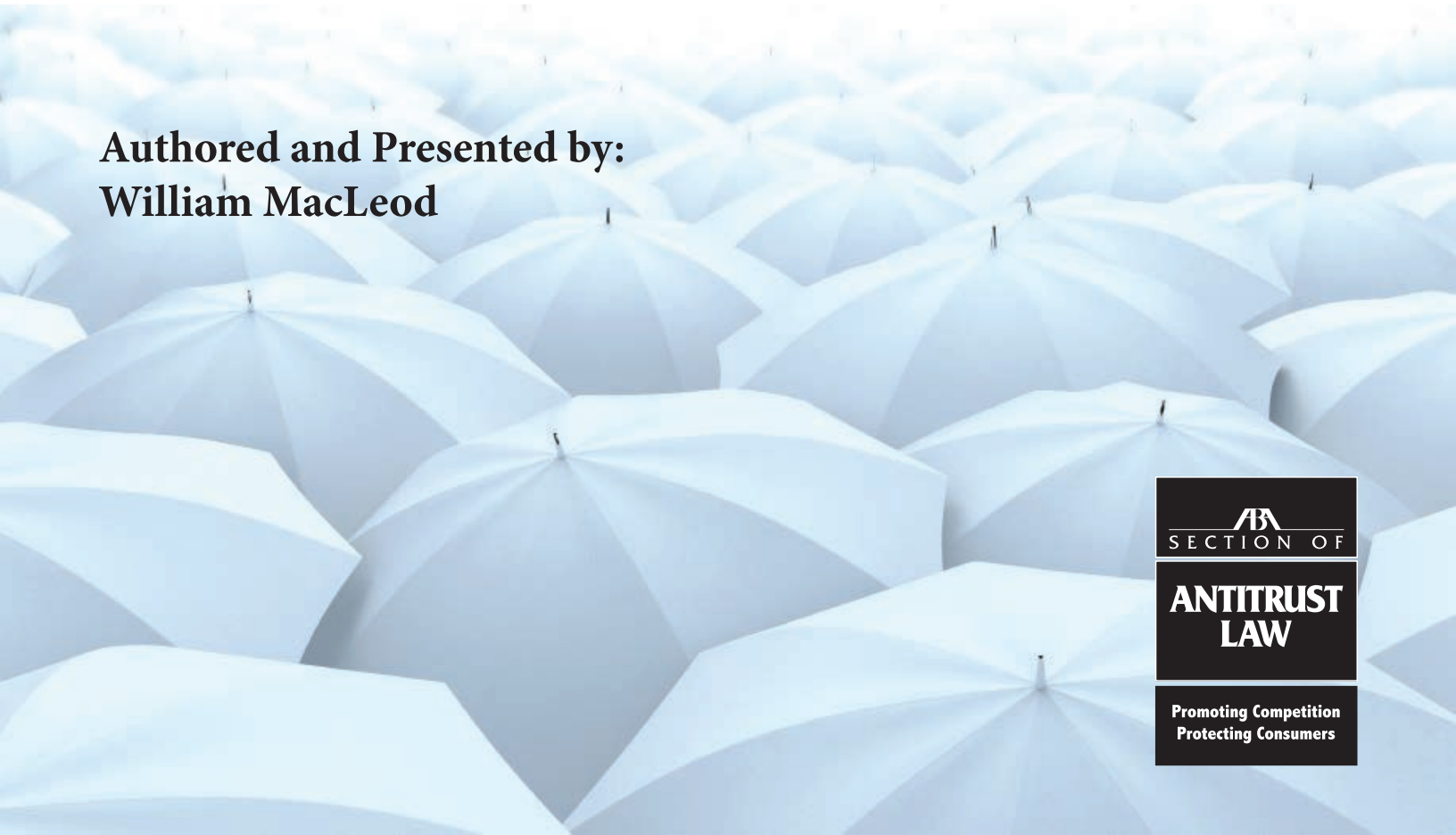
February 7, 2013
9:00 - 9:45 a.m.
Keynote Address: NAAG Presidential Privacy Initiative

2012: A Consumer Protection Year in Review



Authored and Presented by:
William MacLeod

ABA SECTION OF ANTITRUST LAW
Promoting Competition Protecting Consumers

2012: A Consumer Protection Year in Review

William MacLeod

Kelley Drye & Warren

Kelley Drye & Warren LLP
wmacleod@kelleydrye.com

2012: A Consumer Protection Year in Review

It was the biggest year in history for one type of advertising – the pitches for political campaigns. That territory may still be the Wild, Wild West as far as consumer protection is concerned, but agencies, private litigants and companies themselves have turned in a banner year for the consumer.

We will look back on 2012 as a milestone in Consumer Protection. The year began with the appointment of potentially the most powerful cop in the field – the Director of the Consumer Financial Protection Bureau. It ended with the confirmation of the newest Commissioner of the Federal Trade Commission. In between, we witnessed some amazing developments that will change the landscape for as long as we survey it.

So as the country raced from the Iowa Caucuses to the Electoral College to the Fiscal Cliff, the forces of Consumer Protection expanded their reach and asserted new authority. Consumers, we hope, can afford to care a bit less about unfair and deceptive practices in the marketplace. Consumer protection counsel, on the other hand, will have to care a lot more.

Which developments should we care about most? Many candidates are vying for the most important developments of 2012 in Consumer Protection. Ten winners will be announced on February 7, 2013. We will select one from each of ten categories:

1. **Advertising**
2. **Consumer Finance**
3. **E-Commerce**
4. **Economics**
5. **Privacy**
6. **Market Initiatives**
7. **Federal Enforcement**
8. **State Enforcement**
9. **Private Actions**
10. **Constitution**

And we will hazard a prediction of the most important of them all.

The candidates could fill a volume, but the judges have winnowed the list to a few dozen nominees. In the order we saw them appear in 2012, the nominees are:

January

Cordray Appointed to Head CFPB[1]

President Obama started the new year with a recess appointment of Richard Cordray to head the Consumer Financial Protection Bureau ("CFPB"). The President had nominated Cordray as the Director in July, but Senate Republicans blocked Cordray's confirmation. The recess appointment circumventing Senate approval triggered criticism from Republicans, who claimed that the President "arrogantly circumvented the American people" and called the appointment an "extraordinary and entirely unprecedented power grab." Court challenges ensued, but meanwhile, CFPB is on the beat.

FTC Attacks Web-Browsing Toolbar's Privacy Practices[2]

On January 5, 2012, the FTC announced a settlement with Upromise, Inc., a membership service intended to help consumers save money for college, over charges that the company misled users about the extent to which it collected and transmitted their personal information through a "Personalized Offers" feature on a web browser toolbar, and then failed to adequately secure the user information that it collected. Invoking the still powerful tool of challenging a company's descriptions of its policies, the FTC claimed that Upromise's alleged actions were unfair and deceptive and violated the FTC Act.

The FTC alleged that Upromise provided a membership service that allows users to contribute to a college savings account by collecting rebates that are acquired when users purchase goods and services from Upromise partner merchants. Upromise offered users a downloadable web browser toolbar that highlighted Upromise's partner merchants appearing in a user's search results, thereby allowing users to more easily identify merchants that provide the college-savings rebates.

According to the FTC Complaint, when users enabled the "Personalized Offers" feature, the toolbar collected and transmitted the names of the websites visited by users and the links that were clicked on by users, as well as information that users entered into websites, including search terms, user names and passwords, and financial transaction information. The Commission also took issue with security safeguards Upromise used to protect the personal information it transmitted.

---

[1] *See* Thompson, Cordray Gets Recess Appointment to Head CFPB, January 5, 2012.

[2] *See* Hutnik, 2012 Signals Continued FTC Privacy Scrutiny: Web Browser Toolbar Triggers Enforcement Action, January 6, 2012.

Zip Codes Ruled Personally Identifiable Information[3]

A June 2011 lawsuit filed against Michaels Stores Inc. ("Michaels") accused the arts and crafts retailer of violating a Massachusetts consumer protection statute when it collects and records zip codes during consumer credit card transactions. A Massachusetts District Court gave Michaels a new year's gift by granting its motion to dismiss the lawsuit after finding that the plaintiff failed to show cognizable injury. But it was a gift with a catch.

In Tyler v. Michaels Stores Inc., the plaintiff made a purchase at a Michaels store with her credit card and, during the sales process, the cashier requested the plaintiff's zip code. The plaintiff provided her zip code to the cashier allegedly based on the belief that it was necessary to complete the transaction. According to the plaintiff, Michaels then combined her zip code with other information to obtain her home mailing address, and began sending unwanted marketing materials. The plaintiff argued that the collection and recording of zip codes during a credit card transaction violates Mass. Gen. Laws ch. 93 § 105, under which a business cannot "write, cause to be written or require that a credit card holder write [PII], not required by the credit card issuer, on the credit card transaction form."

In its order dismissing the case, the Court determined that a zip code is PII under §105. Specifically, the Court noted that a Massachusetts criminal statute concerning identity theft defines PII as any "number" used "alone or in conjunction with any other information" to assume the identify of an individual. According to the Court, zip codes fit within this definition and are no different than PIN numbers used in debit card transactions because both numbers could be used fraudulently to assume the identity of the card holder when the numbers are recorded on the credit card transaction form.

Despite the Court's determination that zip codes are PII, the Court dismissed the case after finding that the plaintiff could not show that she was injured by Michaels' conduct.

HP Pays $425,000 CPSC Penalty[4]

The Consumer Product Safety Commission ("CPSC") announced that Hewlett-Packard Company has agreed to pay a $425,000 civil penalty to settle allegations that the company failed to report safety issues with its lithium-ion battery pack to the CPSC in a timely manner.

Section 15(b) of the Consumer Product Safety Act requires companies to report immediately to the CPSC if they have information that a product could create a "substantial product hazard" or create an unreasonable risk of serious injury or death. The CPSC alleges that HP was aware of incidents of overheating, two of which allegedly involved injuries to consumers, 10 months

---

[3] *See* Hutnik, Privacy Point of Sale Alert: Massachusetts District Court Finds that Zip Codes Are PII, January 11, 2012.

[4] *See* Richardson, HP Agrees to Pay $425,000 CPSC Penalty, January 24, 2012 (updated Course Set for Higher CPSC Civil Penalties, June 13, 2012).

before reporting to the CPSC. HP and CPSC recalled around 32,000 battery packs in October 2008.

What is most notable about this settlement is that it will look so small compared to what's coming from CPSC. According to a statement released by Chairman Inez Tenenbaum, the settlement with HP was negotiated under the pre-CPSIA enforcement scheme, which had much lower statutory limits on civil penalties. Tenenbaum indicated an expectation that the Commission's future enforcement actions will "include civil penalty amounts that maximize the likelihood of deterring violations."

February

The Best Commercials from Super Bowl XLVI?[5]

HONDA • Matthew's Day Off

"Borrowed interest? Sure. But this commercial had everything you want in a Super Bowl spot—a concept that set the Internet on fire and an execution that was pitch-perfect. Congrats to RPA." Or…

CHRYSLER • It's Halftime in America

"Beautifully crafted, with the hard-boiled performance of the night by Clint Eastwood, this was the only spot from Super Bowl XLVI that truly dared to go beyond advertising—to join the national conversation about something bigger. Some people will hate it for that. To us, it was another masterpiece from Wieden + Kennedy."

FTC Warns 6 Mobile Apps about Possible FCRA Violations[6]

The FTC warned marketers of six mobile apps that provide background screening that the companies may be violating the Fair Credit Reporting Act (FCRA). The FTC warned the apps marketers that, if they believe that the background reports (which included criminal record histories) generated by their apps are being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA.

The FTC sent these warning letters to Everify, Inc., marketer of the Police Records app, InfoPay, Inc., marketer of the Criminal Pages app, and Intelligator, Inc., marketer of Background Checks, Criminal Records Search, Investigate and Locate Anyone, and People Search and Investigator apps.

---

[5] *See Adweek*, The Five Best Commercials of Super Bowl XLVI, available at http://www.adweek.com/news/advertising-branding/5-best-commercials-super-bowl-xlvi-138088, February 6, 2012.

[6] *See* Hutnik, FTC Warns 6 Mobile Apps about Possible FCRA Violations, February 7, 2012.

The warning letters serve as a reminder that broader enforcement by the FTC of the mobile apps sector is likely to follow if mobile app providers engaged in similar practices do not take steps to comply with the FCRA.

Under the FCRA, businesses that assemble or evaluate information that can be considered a "credit report" and provide it to third parties can qualify as consumer reporting agencies. Many companies are often surprised to learn that the information they assemble and/or evaluate and provide to a third party may be considered a "credit report."

These can include drug testing, driving records, among other information, that bears on the character, general reputation, personal characteristics, or mode of living of a person, which is used or expected to be used as a factor in establishing a person's eligibility for employment purposes (among other purposes outlined in the FCRA). For these reasons, close attention should be paid to exactly what information a mobile app provider is assembling and/or evaluating, and how the app provider expects others to use that information, to determine if the FCRA is triggered.

FTC Report Raises Privacy Questions About Mobile Apps for Children[7]

Not an agency to send Valentine's greetings, the FTC instead issued a mid-February report showing the results of a survey of mobile apps for children. These apps can automatically collect a broad range of information, including a user's location, phone number, contacts, call logs, and unique identifiers. However, the report notes that neither the app stores nor app developers provide the information parents need to determine what data is collected from children or how it is shared.

FTC Chairman Jon Leibowitz asked companies to "step up to the plate and provide easily accessible, basic information, so that parents can make informed decisions about the apps their kids use." Specifically, the report recommends that:

- All members of the "kids app ecosystem" should play an active role in providing key information to parents.

- App developers should provide information about their privacy practices in simple and short disclosures. They also should disclose whether the app connects with social media and whether it contains ads. Third parties that collect data also should disclose their privacy practices.

- App stores also should take responsibility for ensuring parents have basic information. The report notes that the stores provide architecture for sharing pricing and category data, and should be able to provide a way for developers to provide privacy information.

[7] *See* Mon, FTC Report Raises Privacy Questions About Mobile Apps for Children, February 16, 2012.

California Attorney General Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications[8]

The release makes it clear. By the end of February, it was clear 2012 would be a year for mobile apps to grapple with privacy law.

> SAN FRANCISCO – Attorney General Kamala D. Harris today announced an agreement committing the leading operators of mobile application platforms to improve privacy protections for millions of consumers around the globe who access the Internet through applications ("apps") on their smartphones, tablets and other mobile devices.
>
> Attorney General Harris forged the agreement with six companies whose platforms comprise the majority of the mobile apps market: Amazon, Apple, Google, Hewlett-Packard, Microsoft and Research In Motion. These platforms have agreed to privacy principles designed to bring the industry in line with a California law requiring mobile apps that collect personal information to have a privacy policy. The majority of mobile apps sold today do not contain a privacy policy

FTC Issues Final Privacy Report[9]

On March 26, the Federal Trade Commission released its much anticipated final Privacy Report, entitled Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. The final report calls on companies to implement best practices to protect consumers' private information (both on- and off-line), Congress to enact baseline privacy and data security legislation with civil penalties, and industry to accelerate the pace of self-regulation. The Report also supports legislation to provide consumers with access to information stored by data brokers and the opportunity to dispute the accuracy of such data.

The Privacy Report also explains that policymakers have a role in assisting with the implementation of self-regulatory principles in the following five key areas, which the FTC will focus on over the next year:

> •Do Not Track: The FTC will be working with relevant stakeholders in completing implementation of an easy-to-use, persistent, and effective Do Not Track system.

---

[8] *See* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy, Release, February 22, 2012.

[9] *See* Hutnik, The FTC's Final Privacy Report, March 26, 2012 (updated in Mobile App Developers Targeted By The California Attorney General's Office, October 31, 2012); *See also* Sullivan, California AG Files Lawsuit Against Delta Airlines For Noncompliance With California's Online Privacy Law, December 7, 2012.

•Mobile: The FTC calls on companies providing mobile services to work towards improved privacy protections, including the development of short, meaningful disclosures. As part of this effort, FTC staff will host a workshop on May 30, 2012 that will address, among other issues, mobile privacy disclosures, and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

•Large Platform Providers: To the extent that large platform providers, such as ISPs, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, the FTC notes its privacy concerns. FTC staff will host a public workshop in the second half of 2012 to further explore privacy and other issues related to this type of comprehensive tracking.

•Promoting Self-Regulatory Codes: FTC Staff will work with the Department of Commerce in facilitating the development of industry-sector specific codes of conduct. To the extent that robust privacy codes of conduct are developed from such efforts, the Commission will view adherence to such codes favorably in connection with its law enforcement work, and will also enforce actions under Section 5 of the FTC Act where companies fail to abide by self-regulatory programs they join.

•Data Brokers: The Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could identify themselves to consumers and describe how they collect and use consumer data, and detail the access rights and other choices they provide with respect to the consumer data they maintain.

Ohlhausen Confirmed as an FTC Commissioner[10]

On Thursday, March 19, 2012, the United States Senate unanimously confirmed Maureen Ohlhausen as a Commissioner of the Federal Trade Commission ("FTC"). Ms. Ohlhausen is a seasoned attorney who has handled consumer privacy and data security issues in public service and private practice, and her confirmation suggests that the FTC will continue to emphasize these areas of the law.

Ms. Ohlhausen was nominated by President Obama in July 2011 to replace Republican William Kovacic, whose term expired in September 2011. As one of five Commissioners, Ms. Ohlhausen will have a seven-year term.

Ms. Ohlhausen returned to the FTC, where she served for eleven years, including a four-year tenure as Director of the Office of Policy Planning. In this role, Ms. Ohlhausen addressed a variety of high-tech legal and policy issues, including barriers to electronic commerce, and online merchants' use of consumer data. In addition, she headed the FTC's Internet Access Task Force.

[10] *See* Istrail, Maureen Ohlhausen Unanimously Confirmed as an FTC Commissioner, January 30, 2012.

April

Groupon Compensates Class Action Plaintiffs for Expiring Gift Cards[11]

Groupon settled a class action alleging its deals violated California and federal gift card laws. The plaintiffs argued that Groupon's deals constituted gift cards, and that the expirations on the deals violated federal and state laws that restrict expiration dates.

Under the proposed settlement, class members who purchased Groupon vouchers between November 2008 and December 1, 2011 will be able to redeem expired vouchers, and if they are unable to do so, obtain a refund from an $8.5 million settlement fund. If a merchant refuses to redeem a settlement voucher, the class member will be entitled to receive a refund of the purchase price plus 20% of the promotional value.

Groupon also agreed to make changes to how it structures and advertises its deals. For example, Groupon agreed to clearly and conspicuously that any expiration dates apply only to the promotional value of the deal, and that the purchase price portion of the deal does not expire until the voucher is redeemed or refunded. And they agreed to limit the number of its annual Daily Deals that expire less than 30 days from the date of issuance.

Google Facing Trial in YouTube Copyright Infringement Suit[12]

The Second Circuit Court of Appeals issued an opinion in the ongoing copyright dispute between Viacom and YouTube/Google. In 2006, Viacom filed a $1 billion lawsuit against Google, alleging that tens of thousands of videos submitted by users and displayed on YouTube violated Viacom's copyrights, and that Google should be liable for the infringement.

In 2010, a federal district court granted Google's motion for summary judgment, holding that Google was entitled to take advantage of the safe harbor provision under the Digital Millennium Copyright Act ("DMCA"). The DMCA safe harbor provision limits the liability of online service providers for copyright infringement that occurs due to a third party's storage of infringing material on the online service provider's system, provided that certain requirements are met. The service provider (1) must not have knowledge of the infringing activity (actual knowledge or "red flag"--awareness of facts or circumstances from which infringing activity is apparent); (2) must not receive a financial benefit directly attributable to the infringing activity; and (3) upon notice from the copyright owner, must take down the infringing content.

Viacom appealed the District Court decision, claiming that Google did not satisfy all of the requirements under the DMCA safe harbor. In its ruling, the Second Circuit vacated the order granting summary judgment, stating that a reasonable jury could find that Google had actual knowledge or awareness of specific infringing activity on its website based on emails and internal documents at Google. The Second Circuit remanded the case back to the District Court.

---

[11] *See* Mon, Groupon Reaches Settlement in Gift Card Lawsuits, April 5, 2012.

[12] *See* Loeffler, Appellate Court Vacates Summary Judgment for Google in Copyright Infringement Suit, April 10, 2012.

The Second Circuit's opinion identifies three types of knowledge that may cause a service provider to lose protection under the safe harbor:

> •Actual knowledge or awareness of specific infringing material--Based on the subjective knowledge of specific infringement;
>
> •"Red Flag" knowledge--Based on awareness of facts that would have made the specific infringement objectively obvious to a reasonable person; or
>
> •Willful blindness to specific infringing activity--The Court held that the willful blindness doctrine could be applied in appropriate circumstances to demonstrate knowledge or awareness of specific instances of infringement.

The Court also addressed the issue of whether Google had the right to control and benefit from the infringing activity, concluding that the standard requires something more than the ability to remove or block access to materials posted on a service provider's website, but remanding the issue for the District Court to determine what is "something more."

The Second Circuit's opinion continues to define the scope of the DMCA safe harbor, while key issues are yet to be resolved by the District Court. Companies engaging in social media, especially the use of user-generated content, should continue to watch this case.

May

MySpace Settles FTC Charges of Misleading Privacy Policy[13]

On May 8, 2012, the Federal Trade Commission (FTC) announced its settlement with social networking service MySpace on charges that it misrepresented its protection of users' personal information in violation of federal law. Like many of its social media counterparts who were recently the target of FTC enforcement actions, Myspace is charged with espousing strict privacy measures and then failing to do as promised.

The MySpace social network comprises millions of users who create and customize online profiles. MySpace assigns a persistent unique identifier, called a "Friend ID," to each profile created. Though users have the ability to upload extensive personal information to their profile, MySpace designates a subset of personal user data as "basic profile information," which include the user's profile picture, Friend ID, location, gender, age, display name, and full name. According to the complaint, this basic profile information is publicly displayed by default and is outside the scope of the privacy settings. The only piece of basic information that users can hide from public view - provided that they change the default setting - is their full name. As of July 2010, only 16% of users had actually changed the default setting to hide their full name.

Under its privacy policy, MySpace promised that it would not share users' personal information or use it in a way that was inconsistent with the purpose for which it was submitted without their

[13] *See* Schiavetti, MySpace Settles FTC Charges of Misleading and Deceptive Statements in its Privacy Policy, May 8, 2012.

consent. In addition, MySpace promised that customized ads would not individually identify users to third parties and would not share non-anonymized browsing activity. According to the complaint, MySpace in fact shared the Friend ID, age, and gender of users with third-party advertisers. Advertisers allegedly used the Friend ID to locate the user's MySpace profiles to obtain personal information, including in most instances the user's full name. Advertisers allegedly could also combine the user's real name and other personal data with additional information to link broader web-browsing activity to a specific individual. In addition, MySpace certified in its privacy policy that it complied with the U.S.- EU Safe Harbor Framework, which provides a method for U.S. companies to transfer personal data lawfully from the European Union to the United States. These statements of compliance were false, according to the FTC.

The order prohibits such practices and requires that MySpace establish a comprehensive privacy program designed to protect users' information, and to obtain biennial assessments of its privacy program by independent, third-party auditors for twenty (20) years.

Skechers to Pay $40 Million Over Allegedly Unsubstantiated Claims for Toning Shoes[14]

Following a similar case last year in which Reebok had agreed to pay $25 million to settle charges that it had made unsubstantiated claims for its toning shoes, the FTC announced that Skechers would pay a record $40 million to settle charges that it made unfounded claims that its toning shoes would help people lose weight, strengthen and tone their muscles, and improve cardiovascular health.

Under the settlement, Skechers is barred from making certain claims for its shoes, unless the claims are backed by "competent and reliable scientific evidence." As with other recent settlements, the FTC describes what evidence is required. For example, for strengthening claims, the company needs "at least one adequate and well controlled human clinical study of the [products] that conforms to acceptable designs and protocols, is of at least six-weeks duration, and the result of which, when considered in light of the entire body of relevant and reliable scientific evidence, is sufficient to substantiate that the representation is true." Other claims require different levels of support.

Not only did the FTC raise the bar on the type of substantiation needed to support certain types of claims, the agency also raised the stakes with higher sanctions for missing the bar.

ALJ Condemns POM Advertising and Disappoints FTC Prosecutors[15]

On May 17, Chief Administrative Law Judge Michael Chappell issued his Initial Decision in the FTC's case against POM Wonderful. The decision found that POM, its parent and its principals violated the FTC Act by making unsubstantiated claims that its pomegranate juice and pills can prevent, treat, cure or mitigate heart disease, prostate cancer, erectile dysfunction, and other medical conditions.

---

[14] *See* Mon, Skechers Agrees to Pay $40 Million to Settle Charges of Unsubstantiated Claims for Toning Shoes, May 17, 2012.

[15] *See* Horvath, Administrative Judge in FTC versus POM Wonderful Lowers the Bar, but POM Still Can't Clear It, May 23, 2012.

On the evidentiary standard to be applied to claims that a food product prevents, treats, mitigates or cures diseases, Judge Chappell ruled that the FTCA does not require an advertiser to have either (1) prior FDA approval of the product for treating such diseases or (2) at least two solid, randomized clinical trials, as would normally be required for FDA approval of a new drug. The judge instead held that substantiation depends on the specific facts and on what experts in the field would consider adequate. He relied on past Commission case law (e.g., In re Pfizer, Inc., 81 F.T.C. 23 (1972); FTC v. Direct Marketing Concepts, Inc., 624 F. 3d 1 (1st Cir. 2010); Removatron Int'l Corp. v. FTC, 884 F.2d 1489 (1st Cir. 1989)) and on the status of pomegranate juice as a non-hazardous food that is not marketed as a substitute for other medical treatment. In certain cases, he conceded, the FTC's flexible standard might parallel that of the FDA. See, e.g., FTC v. Nat'l Urological Group, 645 F. Supp. 2d 1167 (N.D. Ga. 2008).

Even under the flexible substantiation standard, however, POM could not support claims in about half the challenged ads. Some of these advertisements were also found to make deceptive "establishment claims" that touted the existence of scientific or clinical proof of the health benefit. POM appealed its disappointments. So did Complaint Counsel.

June

Spokeo Agrees to Pay $800,000 to Settle Charges of FCRA Violations[16]

Today, the Federal Trade Commission (FTC) announced that Spokeo, Inc., an information broker that markets and sells detailed consumer data profiles, will pay $800,000 to settle FTC charges that it violated the Fair Credit Reporting Act (FCRA).

In its complaint, the FTC alleged that Spokeo sold consumer profiles compiled from Internet and social networking sites, as well as offline data sources, to employment industry professionals as a tool to screen job applicants. The FTC alleged that these profiles were "consumer reports" and Spokeo operated as a "consumer reporting agency."

The FTC alleged that Spokeo violated FCRA by failing to (1) verify who its users are and whether the consumer reports would be used for a permissible purpose, (2) ensure the accuracy of consumer reports, and (3) inform users of their duty under FCRA to notify consumers if the information in the consumer report served as the basis of the user's adverse action against the consumer. The FTC also alleged that Spokeo's online endorsements were deceptive under Section 5 of the FTC Act, as they were provided by Spokeo's employees and not customers. In addition to paying an $800,000 civil penalty, Spokeo agreed to injunctive relief and compliance reporting for 20 years.

[16] *See* Loeffler, Spokeo Agrees to Pay $800,000 to Settle Charges of FCRA Violations, June 12, 2012.

FTC Charges Wyndham Hotels for Alleged Data Security Flaws at Franchisee Locations[17]

On June 26, 2012, the Federal Trade Commission ("FTC") sued global hospitality company Wyndham Worldwide Corporation and three of its subsidiaries alleging that the companies engaged in unfair and deceptive practices by failing to implement adequate data security protections on computer systems located at 90 Wyndham-branded hotels owned by independent licensees.

The Complaint, filed in U.S. District Court in Arizona, claims that the failure to implement reasonable data security safeguards at the franchisee locations allowed computer hackers to breach computer systems and the Wyndham hotel data center on three separate occasions and gain access to the financial account information for more than 600,000 hotel customers. The Complaint also claims that the defendants' privacy policy misrepresented the extent to which the company protected consumers personal information. The Complaint seeks injunctive relief as well as monetary relief for the affected hotel customers.

The FTC's Complaint is significant for two reasons:

> First, it represents the first time that the FTC will litigate its theory as to whether an entity's privacy and data security practices were deceptive and unfair under Section 5 of the FTC Act (past FTC cases have resulted in pre-litigation settlements or informal closings of investigations).
>
> Second, the lawsuit reflects the FTC's effort to hold a corporate brand responsible under the FTC Act for the privacy and information security practices of franchisees and affiliated third parties.

July

GlaxoSmithKline Pleads Guilty and Pays $3 Billion for Promoting Off Label Use and Failing to Report Safety Data

The drug company paid $1 billion in criminal fines and $2 billion to resolve civil liabilities in the government's largest sanction so far against a company that promotes a use of a drug that was not approved by the FDA.[18] The government called the promotion fraudulent.

NAD Determines that Pinterest Promotion Needs Disclosures[19]

The NAD reviewed weight-loss success stories on Nutrisystem's Pinterest board, and determined that the weight-loss claims featured atypical results. The FTC's Endorsement Guidelines state that if an endorser's experience does not reflect what consumers will generally achieve, the ad

---

[17] *See* Hutnik, Complaint Holds Wyndham Hotels Accountable for Alleged Data Security Flaws at Independent Franchisee Locations, June 28, 2012.

[18] *See* Release, GlaxoSmithKline to Plead Guilty and Pay $3 Billion to Resolve Fraud Allegations and Failure to Report Safety Data, available at http://www.justice.gov/opa/pr/2012/July/12-civ-842.html, July 2, 2012.

[19] *See* Mon, NAD Determines that Pinterest Promotion Needs Disclosures, July 13, 2012.

"should clearly and conspicuously disclose the generally expected performance in the depicted circumstances." Accordingly, the NAD held that the Pinterest board should have included a disclosure with the typical weight-loss results.

The NAD's decision contains two important lessons. First, claims on social media sites are still considered advertisements and, therefore, subject to advertising laws. And, second, advertisers should exercise caution when advertising atypical results.

CFPB Withdraws $140 Million From Capital One for Credit Card Marketing

CFPB did not start small. Capitol One became the subject of the agency's first enforcement effort. As its release described to the world, [20] the CFPB took issue with many practices:

> WASHINGTON, D.C. – Today, the Consumer Financial Protection Bureau (CFPB) announced its first public enforcement action with an order requiring Capital One Bank (U.S.A.), N.A. to refund approximately $140 million to two million customers and pay an additional $25 million penalty. This action results from a CFPB examination that identified deceptive marketing tactics used by Capital One's vendors ….
>
> "Today's action puts $140 million back in the pockets of two million Capital One customers who were pressured or misled into buying credit card products they didn't understand, didn't want, or in some cases, couldn't even use," said CFPB Director Richard Cordray. "We are putting companies on notice that these deceptive practices are against the law and will not be tolerated."
>
> Through the supervision process, CFPB's examiners discovered Capital One's call-center vendors engaged in deceptive tactics to sell the company's credit card add-on products. …
>
> Consumers with low credit scores or low credit limits were offered these products by Capital One's call-center vendors when they called to have their new credit cards activated. As part of the high-pressure tactics Capital One representatives used to sell these add-on products, consumers [allegedly] were:
>
> •Misled about the benefits of the products: Consumers were sometimes led to believe that the product would improve their credit scores and help them increase the credit limit on their Capital One credit card.
>
> •Deceived about the nature of the products: Consumers were not always told that buying the products was optional. In other cases, consumers were wrongly told they were required to purchase the product in order to receive full information about it, but that they could cancel the product if they were not satisfied. Many of these consumers later had difficulty canceling when they called to do so.…
>
> •Misinformed about cost of the products: Consumers were sometimes led to believe that they would be enrolling in a free product rather than making a purchase.
>
> •Enrolled without their consent: Some call center vendors processed the add-on product purchases without the consumer's consent. Consumers were then automatically billed for the product and often had trouble cancelling the product when they called to do so.

[20] *See* http://www.consumerfinance.gov/pressreleases/cfpb-capital-one-probe/, Release, July 18, 2012.

Courts Reject Theory that Unsubstantiated Advertising is Deceptive[21]

On July 16, 2012, the United States District Court for the District of New Jersey granted summary judgment in favor of Nestlé Healthcare Nutrition, Inc. in Scheuerman, et al. v. Nestlé Healthcare Nutrition, Inc., No. 2:10-cv-03684 (D.N.J.), a putative nationwide class action challenging Nestlé's advertising and marketing campaign for its BOOST® Kid Essentials Drink ("BKE") product. BKE is a nutritionally complete drink supplement for children, which formerly was sold in a carton attaching a separately-packaged straw containing the probiotic, Lactobacillus reuteri.

In Scheuerman, the plaintiffs alleged that Nestlé committed common law negligent misrepresentation and violated the New Jersey Consumer Fraud Act ("NJCFA"), California's Unfair Competition Law ("UCL"), False Advertising Law ("FAL"), and Consumer Legal Remedies Act ("CLRA"), and Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). They argued that Nestlé made express and implied claims that BKE provided a number of health benefits, including, among other things, immunity protection; a strengthened immune system; reduced absences from daycare or school due to illness; reduced duration of diarrhea; and protection against cold and flu viruses. They also claimed that Nestlé advertised that those challenged health benefits were "clinically shown."

The court held that the plaintiffs could not prevail on their NJCFA, UCL, FAL, or CLRA claims on their theory of liability – that Nestlé lacked substantiation for the challenged advertising claims at the time the claims were made (sometimes referred to as the "prior substantiation doctrine"). Rather, the plaintiffs were required to come forward with evidence actually demonstrating that the challenged advertising claims were affirmatively false, not merely that the claims were not supported by competent and reliable scientific evidence.

This is not the first time a court has rejected the argument that a lack of substantiation amounts to deception. Earlier this year, a Federal District Court in California reached the same conclusion, holding that an alleged lack of substantiation for an advertising representation is not sufficient to state a claim for violation of the California Unfair Competition Law ("UCL") or Consumer Legal Remedies Act ("CLRA"), or for breach of express warranty.[22]

---

[21] *See* Blynn, Federal Court Awards Summary Judgment to Nestlé in False Advertising Class Action Involving Probiotic Supplement, July 25, 2012;

[22] *Stanley v. Bayer Healthcare, LLC*, No. 3:11-cv-00862, 2012 WL 1132920 (S.D. Cal. Apr. 3, 2012); *see generally,* Blynn, Recent Decision Applies Prior Substantiation Doctrine to Bar False Advertising Claims Based on Lack of Substantiation, April 30, 2012.

August

FTC Closes Window on "Up-To" Claims

Diligent readers of the FTC's studies, complaints and orders might have predicted this press release:[23]

> **FTC Warns Replacement Window Marketers to Review Marketing Materials; Energy Savings Claims Must Be Backed by Scientific Evidence**
>
> The Federal Trade Commission warned 14 window manufacturers and one window glass manufacturer that they may be making unsupported energy savings claims for replacement windows. …
>
> Each letter states that the FTC reviewed the company's website and found claims similar to those challenged in administrative complaints the FTC filed earlier this year against five companies. Those companies agreed to orders barring them from making exaggerated and unsupported claims about their windows' energy efficiency and how much money consumers could save on their energy or heating and cooling bills by having them installed.
>
> The warning letters highlight claims that consumers will save more than 30 percent on their energy or heating and cooling bills by installing replacement windows. The letters state that the FTC has made no determination whether the companies are violating the law, but urge the recipients to review their marketing materials with the following in mind:
>
> Energy-savings claims must be backed by scientific evidence.
>
> Be specific about the type of savings consumers can expect.
>
> Avoid deception when making "up-to" claims.…
>
> Manufacturers may be liable for misleading or unsubstantiated claims made to dealers or retailers, in addition to claims made directly to consumers.

The warning letters cited earlier actions and a Commission consumer-perception study[24] that concluded "up to" means that all or almost all consumers would get the claimed performance. The announcement of that study included this description of the results:

> [W]hen marketers use the phrase "up to" in claims about their products, many consumers are likely to believe that they will achieve the maximum "up to" results. The study describes what a test group of consumers thought about ads for replacement home windows that purportedly would provide "up to 47%" savings in energy costs.

The consumers reportedly did not take away the impression from the claim of "up to" that the advertised performance would range from some lower level up to the higher level.

---

[23] *See* http://www.ftc.gov/opa/2012/08/windows.shtm, Release, August 29, 2012.

[24] *See*, *FTC Report: Effects of a Bristol Windows Advertisement with an 'Up To' Savings Claim on Consumer Take-Away and Beliefs*, available at http://www.ftc.gov/os/2012/06/120629bristolwindowsreport.pdf.

September

FTC Exterminates Bedbug Claims

The nation faced an infestation of bedbugs, and the market responded, but some marketers got caught in the FTC's Respondent Motel. Cedarcide and its principles, who sold a line of cedar-oil-based liquid products, faced charges that they made:

- false claims that scientific studies prove Best Yet! is effective at stopping and preventing bed bug infestations, and that it is more effective than synthetic pesticides at doing so;
- a false claim that the Environmental Protection Agency has warned consumers to avoid all synthetic pesticides for treating bed bug infestations;
- false claims that scientific studies prove Best Yet! is effective in stopping and preventing head lice infestations.
- false claims that Best Yet! was invented for the U.S. Army at the request of the U.S. Department of Agriculture, and that the USDA has acknowledged the product as the number one choice of bio-based pesticides.[25]

California Puts Social Media Passwords Off Limits for Employers and Schools

Not to be outdone by Maryland and Illinois, which prohibit employers from demanding access to social media passwords in job settings, or by Delaware, which prohibits schools from doing the same at schools, California now covers both. According to Governor Jerry Brown, "The Golden State is pioneering the social media revolution and these laws will protect all Californians from unwarranted invasions of their personal social media accounts."[26]

The Governor's office described the bills this way:

> Assembly Bill 1844...prohibits employers from demanding user names, passwords or any other information related to social media accounts from employees and job applicants. Employers are banned from discharging or disciplining employees who refuse to divulge such information under the terms of the bill.…The bill further stipulates that nothing in its language is intended to infringe on employers' existing rights and obligations to investigate workplace misconduct.
>
> Senate Bill 1349...establishes a similar privacy policy for postsecondary education students with respect to their use of social media. While the bill prohibits public and private institutions from requiring students, prospective students and student groups to disclose user names, passwords or other information about their use of social media, it stipulates that this prohibition does not affect the institution's right to investigate or punish student misconduct.[27]

---

[25] FTC Release, available at http://www.ftc.gov/opa/2012/09/cedarcidermb.shtm, September 10, 2012.

[26] Release, Governor Brown Signs Laws to Protect Privacy for Social Media Users, available at http://gov.ca.gov/news.php?id=17759, September 27, 2012.

[27] *Ibid.*

October

FTC Issues Revised Green Guides[28]

The FTC issued a revised version of their Green Guides that is designed to help marketers ensure that claims about the environmental benefits of their products are truthful and not misleading. In revising the Guides, the FTC modified and clarified existing sections and provided new guidance on claims that were not common when the Guides were last reviewed.

The Green Guides address the following types of claims: (a) general environmental benefit claims; (b) carbon offset claims; (c) certifications and seals of approval; (d) "compostable" claims; (e) "degradable" claims; (f) "free-of" claims; (g) "non-toxic" claims; (h) "ozone-safe" and "ozone-friendly" claims; (i) "recyclable" and "recyclable content" claims; (j) "refillable" claims; (k) "renewable energy" claims; (l) "renewable materials" claims; and (m) source reduction claims.

The Green Guides aren't new regulations, but they describe the types of environmental claims the FTC may or may not find deceptive under Section 5 of the FTC Act. The FTC has brought several actions in recent years related to green claims, and indicated that they would continue to bring these types of actions.

FTC Posts $50,000 Reward for Best Design of a Drone to Kill Robocalls

At the FTC's Robocall Summit on October 18th, Bureau Director David Vladeck announced a novel challenge – a reward of $50,000 for the best technical solution to block illegal robocalls. "The FTC is attacking illegal robocalls on all fronts, and one of the things that we can do as a government agency is to tap into the genius and technical expertise among the public," said Vladeck.[29] Submissions were due January 17, 2013.

FTC Targets Web-Tracking Company for Privacy Practices[30]

The Federal Trade Commission (FTC) announced that Compete Inc., a web analytics company, agreed to settle allegations that it engaged in unfair and deceptive practices by collecting personal data without disclosing the extent of the information it was collecting and failing to honor promises it made to protect the personal data it collected.

In its complaint, the FTC alleged that Compete persuaded consumers to download its tracking software by urging them to join a Consumer Input Panel and promising them rewards in exchange for sharing their opinions about products and services. Once installed, the tracking software automatically collected not only information about consumers' online activity such web pages visited, but also usernames, passwords, search terms, credit card and financial account information, security codes, expiration dates and Social Security numbers. Compete used the

---

[28] *See* Mon, FTC Issues Revised Green Guides, October 2, 2012.

[29] FTC Release, FTC Challenges Innovators to Do Battle with Robocallers, available at http://www.ftc.gov/opa/2012/10/robocalls3.shtm, October 18, 2012.

[30] *See* Wolff, FTC Settlement Targets Web-Tracking Company, October 26, 2012.

consumer data to generate reports that were sold to third parties about improving website traffic and sales.

The FTC alleged that Compete violated Section 5 of the FTC Act by failing to disclose that it would collect more information than just the web pages that consumers visit, and failing to honor assurances that data are stripped of personally identifiable information before transmission and that the company takes reasonable security measures to protect against unauthorized access alteration, disclosure or destruction of personal information. According to the FTC, Compete failed to provide reasonable and appropriate data security, and failed to use readily available measures to mitigate risk to the data.

November

FTC & CFPB Announce Partnership to Warn and Investigate Mortgage Advertisers[31]

The Federal Trade Commission ("FTC") announced that it had, in partnership with the Consumer Financial Protection Bureau ("CFPB"), sent warning letters to 20 real estate agents, home builders, and lead generators, advising them to review their advertisements to ensure compliance with the Mortgage Acts and Practices-Advertising Rule, Regulation N ("MAP-AD Rule") and the FTC Act. The CFPB also sent warning letters to approximately 12 additional mortgage brokers and lenders.

The FTC and CFPB share enforcement authority over non-bank mortgage advertisers and reviewed over 800 mortgage advertisements for compliance with the MAP-AD Rule, which prohibits material misrepresentations in communications regarding the terms of mortgage financing. The agencies were particularly concerned by advertisements that: (1) offered low "fixed" mortgage rates without disclosing significant terms; (2) suggested the advertiser's affiliation with a government agency; and (3) "guaranteed" approval and low monthly payments without disclosing significant terms. Companies found in violation of the Rule face civil penalties.

Both the FTC and CFPB have opened non-public investigations into mortgage advertisers suspected to be in violation of federal law, with the CFPB announcing that it has launched formal investigations into six companies in particular.

Thirty Seven States Obtain $90 Million from GlaxoSmithKline for Drug Promotions

The drug company was not done after paying $3 billion to the United States in July. This settlement dealt with alleged misrepresentations of risk profiles and safety of Avandia, a diabetes drug. The order prohibits GSK from making false, misleading or unsubstantiated claims about diabetes drugs, and from promoting investigational drugs.[32]

---

[31] *See* Thompson, FTC & CFPB Announce Partnership to Warn and Investigate Mortgage Advertisers, November 20, 2012.

[32] *See, e.g.*, Release, Pennsylvania joins 37 other states in $90 million settlement with GlaxoSmithKline, available at http://www.attorneygeneral.gov/press.aspx?id=6716, November 15, 2012.

December

Second Circuit Overturns Off-Label Marketing Conviction On First Amendment Grounds

In *United States v. Caronia* (Dkt. No. 09-5006 cr, December 3, 2012), a 2-1 decision, the Second Circuit held that "the government cannot prosecute pharmaceutical manufacturers and their representatives under the FDCA for speech promoting the lawful, off-label use of an FDA-approved drug."

Applying the First Amendment in a way that could significantly alter the prosecutorial and regulatory landscape in regulated industries, the United States Court of Appeals for the Second Circuit has overturned the conviction of a pharmaceutical sales representative for conspiring to introduce a misbranded drug into interstate commerce, where his prosecution and conviction were based on conversations he had with physicians about off-label uses for an approved drug.

To determine whether that speech was protected under the First Amendment. The Court followed Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980); and Sorrell v. IMS Health, Inc., 131 S. Ct. 2653 (2011). *Central Hudson* had established the rules that govern commercial speech in the modern era, and *Sorrell* applied it to strike down a Vermont law prohibiting the sale or use of prescriber information for a commercial purpose, without the prescriber's consent.

The Court held that prohibiting the truthful promotion of off-label drug usage did not directly advance the government's goals of preserving the efficacy and integrity of the FDA's drug approval process. Moreover, prohibiting off-label marketing interfered with the ability of physicians and patients to receive potentially relevant treatment information, which could undermine the public interest in informed and intelligent treatment decisions.

The Second Circuit also held that prohibiting off-label marketing failed because it was more extensive than necessary to achieve the government's legitimate purposes of federal drug regulations. A wide variety of alternative ways to regulate off-label usage was available to the government, the Court observed.

The majority held opinion closed by stating:

> We construe the misbranding provisions of the FDCA as not prohibiting and criminalizing the truthful off-label promotion of FDA-approved prescription drugs. Our conclusion is limited to FDA-approved drugs for which off-label use is not prohibited, and we do not hold, of course, that the FDA cannot regulate the marketing of prescription drugs. We conclude simply that the government cannot prosecute pharmaceutical manufacturers and their representatives under the FDCA for speech promoting the lawful, off-label use of an FDA-approved drug.

Vladeck Steps Down

The FTC announces a transition at the top of the Bureau:[33]

> **FTC Announces Departure of Consumer Protection Bureau Director David C. Vladeck and Executive Director Eileen Harrington, Appointment of Charles A. Harwood as Acting Director of the Bureau of Consumer Protection and Pat Bak as Acting Executive Director**
>
> Federal Trade Commission Chairman Jon Leibowitz today announced that David C. Vladeck, Director of the FTC's Bureau of Consumer Protection, is leaving the agency on December 31 to return to a faculty position at Georgetown University Law Center, and that Charles A. Harwood, who has been a Deputy Director in the Bureau for the past three years, will serve as Acting Director of the Bureau of Consumer Protection.
>
> "David has been an extraordinarily effective advocate for American consumers. Under his leadership, the Bureau of Consumer Protection has worked tirelessly to respond to, and to anticipate, the risks consumers face in a rapidly changing marketplace," FTC Chairman Jon Leibowitz said. "We are very fortunate that Chuck Harwood will serve as Acting Director. Chuck's experience, insight, and leadership will ensure continued excellence in the Bureau going forward."

FTC Investigates Data Brokers' Collection and Use of Consumer Data[34]

Only those who had not read a report the FTC issued earlier in 2012 were surprised by the Commission's decision to analyze the industry:

> **Commission Issues Nine Orders for Information to Analyze Industry's Privacy Practices**
>
> The Federal Trade Commission issued orders requiring nine data brokerage companies to provide the agency with information about how they collect and use data about consumers. The agency will use the information to study privacy practices in the data broker industry.
>
> Data brokers are companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies. In many ways, these data flows benefit consumers and the economy; for example, having this information about consumers enables companies to prevent fraud. Data brokers also provide data to enable their customers to better market their products and services….
>
> The FTC is seeking details about:
> -the nature and sources of the consumer information the data brokers collect;
> -how they use, maintain, and disseminate the information; and
> -the extent to which …consumers [can] access and correct their information or to opt out of having their personal information sold.

---

[33] *See* http://www.ftc.gov/opa/2012/12/personnel.shtm, Release, December 17, 2012.

[34] *See* http://www.ftc.gov/opa/2012/12/databrokers.shtm, Release, December 18, 2012 (referring to an earlier 2012 FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers).

FTC Amends the Children's Online Privacy Protection Rule (COPPA)[35]

On December 19, 2012, the FTC issued its long-awaited final amendments to the Children's Online Privacy Protection Rule ("COPPA"). COPPA requires commercial websites and online services that are either directed to children under 13 or have actual knowledge that they are collecting personal information from children under 13 to obtain verifiable parental consent before collecting personal information from such children.

The final revisions significantly modify or expand key definitions within the Rule, including the definitions of "operator," "personal information," and "website or online service directed to children," and update the Rule's requirements concerning parental notice and consent, and the existing safe harbor provisions. These changes broaden the scope of online entities subject to COPPA, provide new pathways to compliance, and include new safeguard requirements, including provisions that involve personal data minimization and disposal obligations.

Among the notable changes are these:

- **Applicability –** The Rule covers both commercial websites and online services directed to children that collect personal information from a child, as well any service that targets general audiences if it has actual knowledge that it is collecting or maintaining personal information from a child.

- **Personal information** – will now include screen names, user names, photographs, video and audio files, geolocation information, an expanded definition of persistent identifiers, and mobile unique identifiers.

- **Collects or collection** – now means passive collecting of information as well as mandating the provision of information. Thus, tracking a child's online activity is now covered, as is any information that an operator encourages or prompts someone to provide.

- **Operator** – now includes child-directed websites or online services that integrate outside services, such as software "plug-ins" or advertising networks, that collect personal information from its visitors. Child-directed content providers are strictly liable for personal information collected by third parties through its site.

    - In addition, third party services, such as plug-ins or ad networks, are covered "**co-operators**" when they have actual knowledge that they are collecting information through a child-directed site.

- **Safe Harbor Parental Consent** – 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.

---

[35] *See* Sullivan, FTC Issues Final Amendments to the Children's Online Privacy Protection Rule (COPPA), January 4, 2013.

FTC Praises Food Companies and Finds Kids Eating Better[36]

A year after the FTC gave up on an interagency initiative to set standards for food-marketing self-regulation, the agency issued an encouraging report on the progress that voluntary efforts had achieved, and on the improvements in kids' diets. As the FTC's release put it:

> **FTC Releases Follow-Up Study Detailing Promotional Activities, Expenditures, and Nutritional Profiles of Food Marketed to Children and Adolescents**
>
> *Commends Industry for Progress, Urges Broader Participation and Continued Improvement*
>
> The Federal Trade Commission today announced the results of a comprehensive study of food and beverage industry marketing expenditures and activities directed to children and teens. The study, A Review of Food Marketing to Children and Adolescents: Follow-Up Report gauges the progress industry has made since first launching self-regulatory efforts to promote healthier food choices to kids. It serves as a follow-up to the Commission's 2008 report on food marketing requested by Congress.
>
> The report released today provides a picture of how food companies allocated $1.79 billion on marketing to youth ages 2-17 in 2009. The FTC found that overall spending was down 19.5 percent from 2006, with most of that decrease coming from less spending on television ads to youth. At the same time, food companies stepped up their spending to market to children and teens in new media, such as online, mobile, and viral marketing, by 50 percent.
>
> New to this report is a detailed analysis of the nutritional profile of foods marketed to youth. The analysis suggests that industry self-regulation resulted in modest nutritional improvements from 2006 to 2009 within specific food categories heavily marketed to youth, such as cereals, drinks, and fast food kids' meals….
>
> The Commission also examined food consumption data from outside sources to look for signs that children and teens are changing their diets as food companies shift their marketing expenditures, marketing techniques, or the nutrition content of the food marketed to youth. The report notes that over the past decade, children and teens have reduced their daily caloric intake, as well as their consumption of total fat, sodium, and sugar.
>
> The report further noted that since 2009 many food companies have continued to improve the nutritional profile of their foods by reformulating existing products and introducing new ones. In July 2011, the Children's Food and Beverage Advertising Initiative (CFBAI) – whose member companies accounted for nearly 90 percent of advertising spending on foods marketed to children in 2009 – announced standardized nutrition criteria that will take effect at the end of 2013….

[36] *See* http://www.ftc.gov/opa/2012/12/foodmarketing.shtm, Release, December 21, 2012.

January 2013

Senate Confirms Economist Joshua D. Wright as FTC Commissioner[37]

The Senate unanimously confirmed Joshua D. Wright to replace J. Thomas Rosch as a Republican commissioner of the Federal Trade Commission (FTC). A highly regarded antitrust scholar, Wright is the author of more than 50 scholarly articles and book chapters and co-editor of three books on topics ranging from Competition Policy and Intellectual Property Law to the Intellectual History of Law and Economics. He will be only the fourth economist to serve as FTC Commissioner and the first Commissioner to hold both a JD and PhD.

***

Which of these developments are the most important of 2012? Does an event after midnight New Year's eve count? What then are the rules? That will be up to the judges. [38]

Let the balloting begin!

[37] Schiavetti, Senate Confirms Obama Administration Nominee Joshua D. Wright as New Republican FTC Commissioner, January 2, 2013.

[38] Disclaimer: "up to" the judges, as used herein, means that the judges, in their sole discretion and without notice to any named or unnamed nominee, may select any nominee in any category; may add nominees, categories, and awards at will; may disregard any and all information contained in this document; and may consider material information not disclosed in this document. Any nominee's appearance on this list should not be deemed an endorsement, testimonial or establishment claim with respect to the nominee itself or to the probability of an award. All decisions will be final when announced on February 7, 2013. Debate at the conference will be encouraged and shall be deemed oral argument, which the judges will take into account. There is no right of appeal.