PRIVACY & DATA SECURITY LAW JOURNAL

VOLUME 3 NUMBER 1 DECEMBER 2007

The PRIVACY & DATA SECURITY LAW JOURNAL is published monthly by Sheshunoff Information Services Inc., 805 Fifteenth Street, N.W., Third Floor, Washington, D.C., 20005-2207.
ISSN 1935-0600

HEADNOTE

The FTC Looks at Privacy and Advertising

STEVEN A. MEYEROWITZ

On November 1 and 2, 2007, the FTC conducted a "Town Hall" on behavioral targeting online, the practice of delivering targeted advertising to online consumers. The event, "Ehavioral Advertising: Tracking, Targeting, & Technology," included nine panels composed of representatives from a number of leading online companies, government officials, and privacy advocates discussing the topic from the perspectives of technology, self-regulation, privacy advocacy, and industry.

In our first article, "Assessing Behavioral Targeting: Notes From The FTC Workshop," D. Reed Freeman, Jr., and Alysa Zeltzer Hutnik of Kelley Drye & Warren LLP provide an executive summary of the workshop, and then a complete recap.

One Year Later

The most recent amendments to the Federal Rules of Civil Procedure — those governing the discovery of electronically stored information ("ESI") — have just turned one year old. In promulgating the new ESI rules, the Rules Committee sought to develop and propose amendments to address the qualitative differences between the discovery of paper documents and ESI as well as problems inherently unique to the discovery of ESI.

In our next article, "Federal Rule Of Civil Procedure 26(b)(2)(B) And 'Reasonable Accessibility': The Federal Courts' Experience In The Rule's

First Year," George B. Murr of Beirne, Maynard & Parsons, reviews court decisions over the past year dealing with discovery of ESI under these amendments.

Minnesota Acts

Given the negative publicity and cost associated with large data breaches, several states have turned to the legislature in an attempt to address this problem. Recently, parts of Minnesota Statute 325E.64 — known as "The Plastic Card Security Act" — became effective and Minnesota became the first state to pass legislation intent on forcing merchants to assume liability for their data retention practices.

Michael P. Carlson, a member of the Board of Editors of the *Privacy & Data Security Law Journal* and a partner at the law firm of Faegre & Benson LLP in Minneapolis, and Laura E. Meyer, an attorney at the firm, are the authors of our next article, "Minnesota's New "Plastic Card Security Act": Forcing Merchants To Step-Up Or Pay Out." Here, the authors analyze the statute and explain steps that affected companies should take.

And More….

We have more here, including our "Current Developments" column by columnist Chris Volkmer. We also have an author index and article index for all of the issues in our second year of publication. As we begin the third year of this journal with this issue, we wish you all a Happy, Healthy, and Peaceful New Year!

Steven A. Meyerowitz
Editor-in-Chief
December 2007

Federal Trade Commission Holds Town Hall Meeting on Behavioral Targeting

D. REED FREEMAN, JR., AND ALYSA ZELTZER HUTNIK

This article summarizes the Federal Trade Commission's Town Hall meeting on Behavioral Targeting, which was held on November 1 and 2, 2007, in Washington, D.C. It first provides an Executive Summary of the key issues discussed at the meeting, and the likely next steps by the FTC following the meeting. Then, this article provides more detailed coverage of the two-day event with an overview of the key panels, including speakers and topics, and the overall take-away from each panel discussion.

EXECUTIVE SUMMARY

There were many issues discussed at the Federal Trade Commission's ("FTC") Town Hall meeting on Behavioral Targeting, which was held on November 1 and 2, 2007 in Washington, D.C., but three key issues dominated the discussion:

1. The "Do Not Track List" proposed by a host of advocacy groups;

D. Reed Freeman, Jr., is a partner in the Advertising and Marketing Practice Group of Kelley Drye & Warren LLP. He focuses on all aspects of consumer protection law, including privacy, data security, and breach notification, online and offline advertising, and direct marketing. Alysa Zeltzer Hutnik is an associate with the firm whose practice includes representing clients in all forms of consumer protection matters. In particular, she specializes in advertising, privacy, and data security law. The authors can be reached at rfreeman@kelleydrye.com and ahutnik@kelleydrye.com, respectively.

2. Whether the Network Advertising Initiative's ("NAI") Principles for Online Preference Marketing are still relevant to the types of behavioral targeting used today; and
3. What types of notice and consumer control are appropriate for behavioral targeting, and whether the government should impose any such requirements.

These three issues are described in order in the following sections.

"Do Not Track List" Proposal

The Center for Democracy & Technology ("CDT") and eight other privacy advocacy organizations[1] proposed in written comments that the FTC implement a "Do Not Track List," which:

1. Would require advertisers using persistent identifiers on consumers' computers to register the domain names of their servers with the FTC; and
2. Allow consumers to import the list and block those domains from tracking their online activity through targeted ads.

We believe that the FTC is highly unlikely, on its own general enforcement authority, and without an express Congressional mandate, to adopt the "Do Not Track List" proposal. There is simply not the consumer outcry on this issue as there was regarding telemarketing, which prompted the Commission to establish the Do Not Call Registry. Moreover, there are serious consequences, both foreseeable and unforeseeable, with such a proposal: it could diminish the effectiveness of third party cookies, thereby reducing advertising online. That, in turn, would reduce the availability of free content online, and ultimately could stifle innovation and cause a loss of jobs in the online sector — all of which would likely raise Congressional ire.

The proposed "Do Not Track List," however, could trigger Congressional or state legislative hearings, which may put pressure on regulators to issue some sort of guidance on behavioral targeting to replace the current best practices regime. These hearings could occur as

early as this Spring, when the FTC is expected to release its staff report on the Town Hall meeting.

NAI Principles for Online Preference Marketing

The NAI Principles, the current self-regulatory program for online preference marketing, were hotly debated, but even industry representatives conceded that the Principles are ripe for review. Industry representatives strongly supported continued self-regulation of behavioral targeting and expressed a willingness to discuss collaborative revisions to the NAI Principles and increased participation of behavioral marketers in the NAI. Advocates insisted that NAI Principles are outdated, with some saying that they could be revised to address tracking technologies other than cookies, and others calling for immediate government action to provide uniform regulation and oversight.

Notice and Consumer Choice

Advocates uniformly called for more robust and transparent notice of behavioral targeting practices, and some urged the Commission to adopt an opt-in regime. Even Commissioner Leibowitz said that opt-in is "preferable" and is on his "wish list," but he stopped short of stating that the FTC should require it.

Industry representatives, on the other hand, pointed out numerous innovative means of providing notice and choice options, such as via a link on the ads themselves. Nearly all of the industry representatives believed that these types of advancements indicate that government prescription of notice requirements is unnecessary and premature. Industry representatives were receptive to revisions of current self-regulatory programs, but urged the FTC to tread lightly concerning any broad regulatory action. Much of the online content that consumers enjoy is subsidized by advertising, and drastic regulations could stifle innovation and growth.

Analysis of the Town Hall Meeting by the Media and the FTC

The Media's Reaction

Media coverage of the Town Hall meeting has primarily focused on

the "Do Not Track List" proposal. While some have reported support for the proposal, other commentators have countered that the list is a bad idea that could backfire, and that disclosed privacy practices should be sufficient. The NAI itself issued a strongly-worded press release criticizing the proposal.

The FTC's Reaction

In her concluding remarks, Deputy Director of the FTC's Bureau of Consumer Protection Bureau, Eileen Harrington, stated:

- Behavioral targeting is growing;
- Behavioral targeting is largely invisible to consumers;
- There should be greater transparency and control for consumers, although consumers struggle with a notice and choice structure; and
- There are "very" legitimate concerns on whether data collected for marketing purposes is put to a secondary use, and over the security of the data, even if it is anonymous.

She went on to say that the FTC is looking for a reasonable and flexible approach that would not stifle innovation, that would prevent harm to consumers, that would provide accountability for companies, and that would reduce burdens for consumers in terms of understanding how their data is used and their choices about such use. She stated that the proposed "Do Not Track List" proposal is "encouraging," as are proposals to reform NAI Principles, and to increase consumer education on behavioral targeting. She promised that the FTC will continue to ask questions of companies in an attempt to learn more about behavioral targeting, especially from companies that did not participate in the Town Hall meeting. State attorneys general may enter the debate as well, evaluating the practices under state law.

FTC Commissioner Jon Leibowitz stated that, to him, the practice of monitoring online conduct or sharing consumer information across websites without real notice is disturbing. This statement is significant because it suggests that at least one FTC Commission believes that website privacy policies, in general, are not noticed, read, or understood by consumers.[2]

Commissioner Leibowitz argued that the four core information practices — notice, choice, access, and security — should be followed when engaging in behavioral targeting. To that end, he said that businesses should provide better and more meaningful information, including shorter privacy policies and notices, more opt-in choices, and more competition. He did *not* say that the FTC would require opt-in for behavioral targeting; rather, he stated that avoiding a government mandate on these issues is preferable. He also said that the "Do Not Track List" is "very promising," but he did not suggest the FTC would adopt it.

The FTC's Likely Next Steps

Issue a Staff Report

This report will simply summarize what the panelists at the Town Hall said, but may give clues of what the FTC's enforcement agenda will be in what the Report characterizes as "areas of agreement" among panelists at the Town Hall meeting. FTC managers have previously said that the report will not include calls for legislative action.

Begin Enforcement Actions

The FTC typically brings the easiest and/or most obvious cases first. Accordingly, the FTC may bring its first case against a company engaged in behavioral targeting that claims to be an NAI full compliance member, but that does not, in fact, follow the NAI Principles. The next case may be against a company using behavioral targeting to deliver deceptive ads targeted to vulnerable groups, such as children, elderly consumers, or consumers with health problems.

Issue Guidance or Endorse Revised NAI Principles

It is difficult to predict where the FTC will go after the anticipated initial round of enforcement actions. While it is possible that the FTC will issue guidelines for behavioral targeting, it is more likely that it will endorse a revised set of NAI Principles, or alternative self-regulatory guidelines, which would give new or clearer rules of the road for advertisers.

DETAILED ANALYSIS OF THE FTC'S BEHAVIORAL ADVERTISING TOWN HALL AGENDA

In her opening remarks, FTC Chairman Deborah Platt Majoras stated that the purpose of the Town Hall meeting was for the Commission to explore:

1. The types of information collected in online behavioral targeting;
2. Whether the information is anonymous;
3. How the information is used and shared;
4. Consumers' understanding of behavioral advertising; and
5. Whether there is consumer harm and, if so, how to address it.

Overview of the Town Hall Meeting's Key Participants and Their Comments on Behavioral Advertising

Industry Panelists

Industry panelists included Randall Rothenberg, Interactive Advertising Bureau, and J. Trevor Hughes, Network Advertising Initiative. General themes were the promise of advertising support as central to the innovation process, and industry's general willingness to collaboratively improve current self-regulatory protections with new ideas and solutions.

Key comments by these participants included:

- Randall Rothenberg: Online advertising is the catalyst for a small business renaissance in America. Any regulation beyond the current framework of industry self-regulation and market practices must not curtail advertising support of industry growth.
- J. Trevor Hughes: Layers of protection are built into the Internet to provide consumers with protection and assurance. These protections include privacy policies, browser controls, self regulatory programs, and consumer downloaded programs.

Advocates and Academics

Advocate and academic panelists included Richard M. Smith, Boston Software Forensics, and Jeff Chester, Center for Digital Democracy ("CDD"). General themes were the complex process behind online ad delivery, the gathering of "aggregate statistics," and the CDD complaint filed on November 1, 2007, requesting immediate investigation. The CDD complaint raises concerns over privacy rights in:

1. User tracking/web analytics;
2. Behavioral targeting and retargeting;
3. Audience segmentation;
4. Data gathering/mining;
5. Industry consolidation;
6. Targeting youth online; and
7. Monetizing social networks. It states that industry self-regulation has failed and calls for immediate changes.

In particular, Jeff Chester (the author of several "Complaints"[3] to the FTC that helped spark the FTC's interest in online behavioral targeting noted):

> The core privacy principles identified in a 1998 FTC report — notice, choice, access, and security — need to be redefined.
>
> - "Notice" should indicate what data is being collected, how it is being used, and whether it will be shared with other parties. This should include any data collection practice including cookies and web beacons;
> - "Choice" should apply only on an opt-in basis;
> - "Access" should allow consumers to examine, correct, and/or delete online data collected about them; and
> - "Security" should apply a strict, limited data-retention policy for the storage of personal data, retaining information only for the

duration of a particular task and for a maximum of 6 months, without explicit consumer consent.[4]

Overall Takeaway

In general, participants agreed that the process of delivering a targeted ad to a consumer can be complex and many variables must be considered, but that the concept of behavioral targeting is not new. Participants also agreed that the amount of free content available to consumers is largely due to advertising support.

Participants, however, disagreed on the issues related to privacy and security. Industry members argued that current growth is due to current self-regulatory programs that permit innovation in the industry. Advocates argued that self-regulatory programs have failed, and some advocates called for immediate regulatory and enforcement action.

The Panel on "Behavioral Advertising Today: Understanding the Business and Technology"

Industry Panelists

Industry panelists included Dave Morgan, Tacoda Inc., Robert Gratchner, AQuantive, a subsidiary of Microsoft Corp., Michael Walrath, Yahoo! Inc., Tim Armstrong, Google Inc., Chanterria McGilbra, Netmining, Pam Horan, Online Publishers Association, Mark Westlake, HowStuffWorks.com, and Ralph Terkowitz, ABS Capital Partners.

The general themes discussed during this panel included the:

- Importance of innovation in the market;
- Establishment of privacy policies that inform consumers;
- Use of appropriate privacy practices;
- Ability to deliver relevant, clutter free content to consumers through behavioral targeting, and
- Importance of consumer trust in the business.

Key comments by these participants during this panel included:

- Dave Morgan: Innovation protects privacy by providing more information, better privacy tools, and a better consumer experience. The future is less clutter and more relevant ads;
- Tim Armstrong: Google will continue to work with any group to increase privacy, hopes the FTC will look across the continuum of practices, asks the FTC to tread lightly so as not to slow innovation, and states that privacy and trust are core to the Internet's growth; and
- Mark Westlake: Behavioral targeting allows small publishers to compete with much larger sites.

Advocates and Academics

Carlos Jensen, Oregon State University, commented that:

- He performs research using an iWatch Web Crawler tool that catalogs data collection and privacy practices, including cookies, web beacons, pop-ups, banner ads, privacy policies, and seals; and
- Consumers have limited attention spans, but the number of pages, domains, and countries with online content is increasing. Third party cookie use increased 70 percent in the U.S. (to 5.9 percent of sites), and the use of web beacons has increased.

The FTC's Questions and Panelists' Responses

Is there adequate control for consumers over their profiles?

Industry representatives responded that categorization of consumers is necessary to make ads relevant and valuable. Innovation may allow consumers to edit these profiles, but this is still in testing.

Is opt-in a solution?

Again, industry representatives responded that there is much less free online content in the EU, where opt-in is the rule.

The Panel on "Consumer Survey Data"

Advocates and Academics

George R. Milne, University of Massachusetts-Amherst, commented that consumers have different information exchange expectations depending on the situation, and overall consumers want to control their environment and technology, choosing to restrict more invasive forms of communication.

Dr. Larry Ponemon, Ponemon Institute, commented that:

- Consumers want more control and prefer personalization when it is relevant and interesting. As consumer control over the type or frequency of ads increases, so does their trust;
- The term "cookie" has negative connotations, but there is a downward trend in cookie deletion — perhaps due to complacency or difficulty in removal; and
- Consumers would not pay for online services, even if it would stop online ads.

The Panel on "Data Collection, Use, and Protection"

Industry Panelists

Industry panelists included: Nicole Wong, Google Inc., Diane McDade, Trustworthy Computing, Microsoft Corp., Scott Nelson, TruEffect, and Chris Kelly, Facebook.

The general themes discussed during the panel included the importance of privacy policies and privacy practices built into the web.

Key comments by these participants during this panel included:

- Nicole Wong: Advertising is critical to the web ecosystem, but consumer trust and privacy are paramount because of low switching costs for consumers. A balance between beneficial online ads and protecting consumer privacy must be struck;

- Diane McDade: At Microsoft, privacy practices are imbedded into product design, and audits ensure adherence. Practices are guided by a layered privacy policy with more detailed notice, increased opt-out choice, data retention limits, and security scrubbing of certain PII; and
- Chris Kelly: Privacy is built into the Facebook architecture. Consumers control the collection of information by creating their own profiles. They control use of information by choosing who to share their profiles with — the average user has access to only 0.15 percent of all profiles. Security is regulated by profile availability, confirmation of friends, network rules, encryption of sensitive data, and systems to detect spam.

Advocates and Academics

Amina Fuzlullah, U.S. Public Interest Research Group, commented that data collection begins even before consumers can view products online, which may affect individual prices. Privacy is not based purely on PII, and that even a non-PII profile has value to the industry. She also noted that transparency is lacking because consumers cannot necessarily refuse to provide information online.

The FTC's Questions and Panelists' Responses

Why do data retention practices keep data for one to two years, and is this data accessible by third parties?

Industry responded that data must be retained to provide robust services and maintain system security. Reverse engineering an individual identity would require access to a consumer's computer or information from an ISP. Information that is retained within the business is almost impossible to obtain.

Advocates responded that, if an ISP and tracking company work together, almost nothing is anonymous.

Dr. Ponemon stated that there are different solutions for good and bad actors. A broad regulation could get in the way of progress and result in serious economic consequences. Accordingly, he said, the FTC should tread lightly in regulating behavioral targeting.

What sensitive information is off-limits?

There was no consensus on this issue. Industry representatives noted that it is difficult to draw the line. Health information — relating to HIV/AIDS, cancer — is generally considered off limits, but then it becomes a question of what diseases/ailments are sensitive.

What is the most serious harm possible, and who should act?

Advocates referred to the loss of consumer control and resulting profiles and segmentation. They generally called for increased FTC activity. Industry panelists noted that their view that data security and inappropriate use by bad actors are the main issues. They called for more responsive privacy and security measures, enacted by industry itself, on a global scale.

Overall Takeaway

The participants generally agreed that active deception is wrong, and that there is a need for increased transparency. Security of data — even anonymous data — is key.

There were, however, varying positions by the participants regarding the length of time data must be retained, ranging from days to 18 months. Participants questioned (without much support) whether information is truly anonymous, especially if it is compared across separate databases. In addition, while participants generally agreed that encouraging the entire behavioral targeting industry to get involved in the NAI is positive, advocates called for uniform practices across behavioral targeting implementations and stronger oversight.

The FTC staff noted that its concern is consumer harm, and on this issue, there was no real consensus. Advocates argued that harm could be based on price or other discrimination, taking advantage of vulnerable groups, and inadequately disclosing the practices of behavioral tracking. The FTC did not expressly call any of these "harms."

The Panel on "Disclosures to Consumers"

Industry Panelists

Scott Shipman, eBay Inc., commented that:

- eBay's AdChoice program includes labels on ads with text such as "About," "What's This," or "AdChoice";
- Label links to a page that describes the use of information for ad targeting, and permits an opt-out; and
- If consumers are signed into eBay, they can choose to use information for targeted ads on eBay, or permit sharing anonymized info with others outside the site.

Advocates and Academics

Lorrie Faith Cranor, Carnegie Mellon University, commented that:

- Privacy policies are full of hedging language;
- Studies reveal that consumers could scan policies for keywords, but were less able to analyze protections (i.e., layered notices do not provide much help), and that consumers trust longer policies but like shorter policies; and
- Consumers may be willing to pay a "privacy premium" to buy from those with good privacy practices.

Declan McCullagh, CNET News, commented that search engines can list individuals by IP address or cookie value based on a list of search terms. Alternatively, given an IP address, the search engine can identify the consumer's actions while online.

The FTC's Questions and Panelists' Responses

Do disclosures work, and how can you motivate consumers to search further?

Industry responded that easy access to privacy policies are key, i.e., a

link on every webpage and layered or easy-to-read policies. Industry representatives also discussed a number of innovative notice and choice concepts, including AOL's Consumer Choice initiative, eBay's ad labeling, Google's use of blogs and videos to get their privacy message out, and MSN's use of layered privacy notices.

Should there be specific disclosures for behavioral targeting and how can you improve notice and choice?

Some industry representatives made the point that it is impossible to require consumers to read the privacy statement. TRUSTe raised the possibility of a behavioral targeting seal in the future, but urged continued business experimentation to determine what works.

SafeCount noted its use of a cookie transparency process that allows consumers to research the information collected about them and sent to advertisers. Consumers can set the interaction level. The FTC indicated that this might be a sensible option.

Finally, advocates urged that the process must be simple and inform consumers so that they can make meaningful choices, such as use of something akin to a "nutrition label" that identifies the important aspects of a privacy policy.

Overall Takeaway

Overall, panelists agreed that several companies are testing notice/choice options from a link on the ad itself, which was generally viewed as one among a number of positive options for providing better information. Most of the panelists were not in favor of the government stepping in to prescribe notice requirements.

The panelists disagreed on whether there should be standardized graphical icons or notices. Some panelists also pointed to the length of time necessary to develop new notice and choice regimes, including the necessary time to test what works best.

The Panel on the "Regulatory and Self-Regulatory Landscape"

Industry Panelists

J. Trevor Hughes, Network Advertising Initiative, commented that:

- NAI principles are part of the layers of protection. This includes privacy policies, browser controls, P3P, anti-spyware software, web seals, and certifications. NAI principles were created for a specific function: online preference marketing;
- They provide notice and choice, and special protections for sensitive data; and
- The time is appropriate to review best practices, and the NAI is open to that dialogue.

Advocates and Academics

Pam Dixon, World Privacy Forum, commented that there is a purported failure of the opt-out cookie due to lack of consumer use and its fragility and susceptibility to deletion. She also noted that the World Privacy Forum ("WPF") argues that core protection is not persistent. WPF submitted a report criticizing the NAI Principles, including that consumers have difficulty opting out via the NAI website and that the NAI Principles do not currently address new tracking technologies, such as flash cookies.

The FTC's Questions and Panelists' Responses

Are there other models of self-regulation?

Industry participants (e.g., NAI, Direct Marketing Association, OPA, IAB) commented that companies are competing over privacy, which is a very promising development, and which suggests that the time is not ripe for government intervention. In addition, the Direct Marketing Association ("DMA") has published online marketing best practices and special guidelines for health data. The key, according to industry participants, is to allow multiple forms of self-regulation, and to foster the competition and innovation over privacy that exists today.

Advocates stated that industry guidelines are not working. State Attorneys General responded that states are examining the practices under state consumer protection laws. A representative of the Texas Attorney General commented that transparency is critical.

Overall Takeaway

Generally, participants agreed that all methods of regulation need further exploration, including whether a revision of current self-regulatory programs would provide for greater industry involvement and enforcement, or if the creation of government enforcement mechanisms would be more appropriate.

Participants disagreed on whether a "Do Not Track List" would be a positive development, and questioned whether it would block only targeted ads, all ads, or websites entirely. Industry participants stated that self-regulation continues to work, perhaps with modification, while advocates called for formal regulation of such practices.

FTC staff members commented that they are interested in exploring all methods of protecting consumers, and that the FTC is examining the self-regulatory structure– whether that industry oversight would be by one organization, such as the NAI, or under multiple industry specific self-regulatory programs. The FTC is also interested in learning more about the "Do Not Track List" proposal, including the reach of the proposal, technology and implementation challenges, and its potential effects on commerce. In terms of enforcement, the FTC emphasized several times that its focus is on consumer harm, and the Town Hall meeting failed to produce any consensus on what aspects of Behavioral Targeting (at least performed under the existing NAI Principles) result in concrete harms to consumers.

NOTES

[1] Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse, and World Privacy Forum.

[2] Commissioner Leibowitz cited a study on privacy policies, which revealed

that 1 percent of privacy policies are understood by those without a high school education, only 27 percent allowed consumers to opt-out, and none allowed consumers to opt-in.

[3] The first such "Complaint" was filed on November 1, 2007, exactly one year prior to the first day of the Town Hall meeting.

[4] Note that the CDD's complaint asks the FTC to initiate: an investigation into the companies it cites, a special task force to examine new threats to children and teenagers, an inquiry into the data collection and target marketing practices of social networks, an investigation into the role of behavioral targeting in the subprime mortgage industry, examination of the role of racial profiling and ethnic identification, and an update of FTC privacy principles to comply with OECD guidelines.