FTC Staff Report:

Self-Regulatory Principles For Online Behavioral Advertising

February 2009

invisibility of the data collection to consumers; the shortcomings of current disclosures about the practice; the potential to develop and store detailed profiles about consumers; and the risk that data collected for behavioral advertising – including sensitive data regarding health, finances, or children – could fall into the wrong hands or be used for unanticipated purposes. Following the Town Hall, FTC staff released for public comment a set of proposed principles (the "Principles") designed to serve as the basis for industry self-regulatory efforts to address privacy concerns in this area.

In drafting the Principles, FTC staff drew upon its ongoing examination of behavioral advertising, as well as the public discussion at the Town Hall. Pli(ll.on

reasonably be associated with a particular consumer or computer or other device, regardless of whether the data is "personally identifiable" in the traditional sense. Indeed, in the context of online behavioral advertising, rapidly changing technologies and other factors have made the line betwee

appropriate protections for such data. Relatively few of the commenters answered staff's request for additional info

I. INTRODUCTION

On December 20, 2007, Federal Trade Commission ("FTC" or "Commission") staff released for public comment a set of proposed self-regulatory principles related to online

[1] FTC Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[2] FTC Town Hall, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

A cookie is a small tex

[5] Ads from network advertisers are usually delivered based upon data collected about a given consumer as he or she trave

2000), *available at* 2000), *available at*

[6] *See, e.g.*, FTC Report, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 3-6 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. This report described0 rg72.sslo 31.2000 0.00CH76.2

Recommendations (July 2000) ("July 2000 Report"),[11] supplemented the first report by addressing self-regulatory principles developed by the Network Advertising Initiative ("NAI"). NAI, an organization consisting of online network advertisers, had developed these principles ("NAI Principles") that [illegible] an orgAw0 rgBT10 .0ally)T=/c").c 0.0000 T2p

[11] July 2000 Report, *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf.

[12] Issued in 2000, the NAI Principles required network advertisers to notify consumers about profiling activities on host websites and to give consumers the ability to choose not to participate in profiling. The NAI Principles applied to both personally identifiable and non-personally identifiable consumer data. Where a member collected personally identifiable information, it had to provide notice and opt-out choice at the time and place of collection. For non-personally identifiable information, notice could appear in the publisher website's privacy policy with a link to the NAI website, where a consumer could opt out. The NAI Principles also imposed certain restrictions on the merger of personally identifiable information with non-personally identifiable information. As discussed in more detail below, NAI recently released revised principles.

[13] *See* July 2000 Report, *supra* note 11, at 10-11.

[14] *See, e.g.*, George Raine, *Dot-com Ads Make a Comeback*, S.F. CHRON., Apr. 10, 2005, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/10/BUG1GC5M4I1.DTL (discussing negative impact of dot-com implosion on online advertising generally).

NAINAI

[15] *Id. See also* Ryan Blitstein, *Microsoft, Google, Yahoo in Online Ad War*, SAN JOSE MERCURY NEWS, May 19, 2007.

[16] The complete transcripts of the hearings, entitled *Protecting Consumers in the Next Tech-Ade*, are available at http://www.ftc.gov/bcp/workshops/techade/index.html

See Letter from Jeffrey Chester, Executive Director

[22] Many similar issues arose during the FTC Town Hall held in May 2008 on the mobile commerce marketplace. There, participants discussed consumers' ability to control mobile marketing applications, the challenges of effective disclosures given the size limitations in the mobile context, marketing to sensitive groups, and the developments of the next generation of mobile-based products and services. *See generally* FTC Town Hall, *Beyond Voice: Mapping the Mobile Marketplace* (May 6-7, 2008), *available at* http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

[23] *See, e.g.*, Transcript of Town Hall Record at 144-149, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/71102wor.pdf (statements of Pam Dixon, Executive Director, World Privacy Forum) [hereinafter "Nov. 2 Transcript"].

Id.

in at

et al., *Consumer Rights and Protections in the Behavioral Advertising Sector*, *available at* http://www.cdt.org/pr28w717lh143.8800 0.0000 TD28.71031c(Consupctor)T107143.8800 0.0000 TD Protectib

Staff at to at ll at

[25] *See, e.g., In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf

http://googleblog.blogspot.com/2008/08/new-enhancements-on-google-content.html (Aug. 7, 2008, 5:01 EST).

[29] *See* Gregg Keizer, *Microsoft Adds Privacy Tools to IE8*, COMPUTERWORLD.COM, Aug. 25, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113419. As noted above, a coalition of privacy groups also has proposed and continues to support development of a "Do Not Track List" designed to increase consumer control over the tracking of their online activities. *See* Schwartz et al., *supra* note 24.

[30] *See* AOL, Privacy Gourmet Page, http://corp.aol.com/o/mr-penguin/ (last visited Jan. 9, 2009); YouTub an. 9,

NAI issued proposed principles for public comment in April 2008. *See* NAI,

INFORMATIONWEEK, Jan. 13, 2009, http://www.informationweek.com/news/showArticle.jhtml?articleID=212900156. The IAB, an organization of companies engaged in online advertising, previously issued a set of privacy principles recommending

Privacy Implications of Online Adve

behavioral advertising, staff has ongoing questions about the precise operation of this marketplace, particularly as it continues to develop and evolve. In addition, much remains to be learned about consumers' awareness, attitudes, and understanding of the practices. Staff therefore will continue to examine the issues as the market develops and will propose additional actions as needed. Staff also intends, where appropriate, to initiate investigations of possible unfair or dece

[47] Traditionally, PII has been defined as information that can be linked to a specific individual including, but not limited to, name, postal address, email address, Social Security number, or driver's license number. Non-PII includes anonymous data that, without more, cannot identify a specific person. *See, e.g.*, June 2000 Report, *supra* note 10, at 4 & n.14.

An

[49] *See, e.g.*, July 2000 Report, *supra* note 11, at 11 n.33 (majority of the Commission recommended online privacy legislation applicable to both PII and non-PII); NAI 2008 Principles, *supra* note 32, at 3, 7-8 (since 2000, Principles have provided protections for PII and non-PII); Dingell et al., *supra* note 42 (seeking information from 34 companies on all aspects of their online behavioral advertising practices, regardless of whether the practices implicated PII or non-PII).

[50] In recent years, portable devices with multiple built-in functionalities tied to individual consumers have proliferated. These include devices such as "smart" mobile phones that allow Internet access and email, as well as BlackBerrys and other similar tools. The explosion in the number of devices in use world-wide is rapidly exhausting the available IP addresses required for online connectivity. In order to accommodate this growing demand, the market is undergoing a transition to a new generation of IP addresses – "IPv6." IPv6 will dramaticam12.0300 Tc0.0000 [illegible]

medical conditions and prescription drugs she is researching; when combined, such information would constitute a highly detailed and sensitive profile that is potentially traceable to the consumer. The storage of such data also creates the risk that it could fall into the wrong hands or be used later in combination with even richer, more sensitive, data.[51]

Fourth, in some circumstances, such as when more than one individual in a household shares or has access to a single computer, the distinction between PII and non-PII may have no bearing on the privacy risks at issue. For example, one user may visit a website to find information about a highly personal or sensitive topic, such as the user's health issues or sexual preference. In such circumstances, the delivery of advertising associated with that user's searches to the shared computer, even if the advertising does not identify the user, could reveal private information to another user of the same computer.

Finally, available evidence shows that consumers are concerned about the collection of their data online, regardless of whether the information is characterized as PII or non-PII. Recent survey data suggests that significant percentages of consumers are uncomfortable with

---

[51] This hypothetical is supported by the 2006 incident in which AOL made public some 20 million search queries conducted by thousands of subscribers over a three-month period. After replacing subscriber names or user IDs with identification numbers in order to protect the searchers' anonymity, AOL posted the data for research purposes. The data, which was posted for about a week, connected the "anonymized" AOL member with his or her search queries, the number of websites identified by AOL's search engine as responsive to the search queries, and the responsive website the individual chose to visit. Using this information, the media was able to identify, with little additional investigation, at least one individual subscriber and "bloggers" and other Internet users claimed to be able to identify others. *See, e.g.*, Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&scp=1&sq=aol%20queries&st=cse&oref=slogin; Ellen Nakashima, *AOL Takes Down Site With Users' Search Data*, WASH. POST, Aug. 8, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080701150.html.

having their online activities tracked for purposes of delivering advertisements, even where the data collected is not personally identifiable.[52] Further, many consumers reacted strongly to the AOL incident, described above, in which AOL made public purportedly anonymous data about its subscribers' online ac

[52] *See, e.g.*, Press Release, Consumers Union, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy* (Sept. 25, 2008), *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (over half of respondents uncomfortable with internet companies using their browsing histories to send relevant ads or third parties collecting information about their online behavior); Press Release, Harris Interactive Inc., *Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles* (Apr. 10, 2008), *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=894 (59% of survey respondents were "not comfortable" with online behavioral advertising; however, after being shown model privacy policies, 55% said they would be more comfortable); Press Release, TRUSTe, *TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting* (Mar. 26, 2008), *available at* http://www.truste.org/about/press_release/03_26_08.php (57% of survey respondents "not comfortable" with advertisers using browsing history to serve relevant ads, even when information cannot be tied to their names or other personal information); George Milne, "Information Exchange Expectations of Consumers, Marketing Managers, and Direct Marketers" at 3, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3gmilne.pdf (45% of respondents think online tracking should not be permitted; 47% would permit tracking with opt-in or opt-out rights); *see also* Larry Ponemon, "FTC Presentation on Cookies and Consumer Permissions" at 11, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3lponemon.pdf (only 20% of respondents would voluntarily permit marketers to share buying behavior with third parties to project future buying decisions).

[53] *See, e.g.*, *AOL is Sued Over Privacy Breach*, L.A. TIMES, Sept. 26, 2006, at C2, *available at* http://articles.latimes.com/2006/sep/26/business/fi-aol26; Barbaro & Zeller, Jr., *supra* note 51; Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TechCrunch, Aug. 6, 2006, http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/all-comments/. The AOL incident highlights the difficulties in making data truly anonymous. Simply eliminating name, contact information, or

other traditional PII may not be sufficient. For example, a study conducted in 2000 used U.S. Census summary data to find that 87% of the U.S. population could likely be uniquely identified based only on three pieces of data: a 5-digit zip code; gender; and date of birth. Latanya Sweeney, Abstract, *Uniqueness of Simple Demographics in the U.S. Population* (Carnegie Mellon U., Laboratory for Int'l Data Privacy 2000), *available at* http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html; *see also* Bruce Schneier, *W*

following books"). In such case, the tracking of the consumer's online activities innlie

[55] Staff notes that to the extent that these functions do not involve the tracking of consumers' online activities in order to deliver advertising based on those activities, they do not constitute online behavioral advertising and thus already fall outside the Principles' scope.

3. Applicability to Contextual Advertising

Numerous commenters, representing both industry and consumer groups, recommended that the Commission revise the Principles' behavioral advertising definition to expressly exclude contextual advertising. These commenters explained that online contextual advertising differs from behaviorally targeted advertising because it is based only on the content of a particular website or search query, rather than on information about the consumer collected over time. For example, where a consumer i t

consistent with reasonable consumer expectations. For instance, although one might expect that Citibank and Citifinancial are closely linked entities, the link between affiliates Smith Barney and Citibank is likely to be much less obvious. Such a determination will depend upon the particular circumstances. Staff also notes that the GLB Act does not, in fact, address affiliate sharing among financial institutions; rather, the Fair Credit Reporting Act governs affiliate sharing and allows consumers to opt out of sharing certain data with affiliates. *See* 15 U.S.C. §§ 1681a(d)(2)(A), 1681s-3 (2003).

[61] These commenters cited self-regulatory regimes such as DMA's "Online Marketing Guidelines," IAB's "Interactive Advertising Privacy Principles," and the NAI Principles.

[62] Some commenters also state that encouraging companies to provide choice for the mere *collection* of data is inconsistent with existing legal and self-regulatory regimes, which focus on choice in connection with particular *uses* of data. In fact, the Principles focus on the collection of data *for behavioral advertising*, which presumes both collection and use (or at least intended use) for that purpose. Further, the central goal of the Principles is to minimize potential misuses of data, including uses of data that could cause harm or are contrary to consumer expectations. Nevertheless, because many of the privacy concerns raised about behavioral

In contrast, various consumer and privacy interest groups, as we

advertising relate directly to information *collection* – including the invisibility of the practice and the risk that sensitive data, once collected, could fall into the wrong hands – staff believes that it is important to protect the data at the time of collection.

[63] The proposed Principles do not specify whether this choice would be opt-in or opt-out choice – just that it be clear, easy-to-use, and accessible to consumers. As discussed below, however, the Principles do specify affirmative express consent (opt-in) for uses of data that raise heightened privacy concerns – specifically, material changes affecting the use of previously collected data and the use of sensitive consumer data.

[64] *See supra* note 24.

that consumers are concerned about their data collected online, regardless of whether it is characterized as PII or non-PII. Finally, because staff has clarified that the Principles do not cover "first party" and "contextual" advertising, the costs of providing choice should be significantly less than stated in some comments.

2. Providing Effective Notice and Choice

Many commenters also addressed the issue of *how* businesses engaged in behavioral advertising should notify and offer choice to consumers concerning the collection and use of their data. Several companies stated that the appropriate location for any disclosure regarding online behavioral advertising is the website's privacy policy, and suggested that additional or alternative mechanisms for such disclosures could confuse consumers or encumber online functions. These commenters argued that consumers expect to find information on data practices in privacy policies and that this existing framework effectively informs consumers. Other companies and some privacy advocates highlighted the need for additional disclosure mechanisms beyond the privacy policy and suggested various options, such as: (i) providing "just-in-time" notice at the point at which a consumer's action triggers data collection; (ii) placing a text prompt next to, or imbedded in, the advertisement; and (iii) placing a prominent disclosure on the website that links to the relevant area within the site's privacy policy for a more detailed description.

A number of consumer and privacy groups' c

that the use of standard or uniform disclosures would make disclosures more effective and would increase consumers' understanding of data collection practices. A group of privacy and consumer advocates recommended that, where a consumer opts out of behavioral advertising, companies should honor that choice until the consumer decides to opt in and should not attempt to circumvent the consumer's choice through technological means. These commenters also called on companies to allow consumers to view and change their choices at any time.

he

[65] *See supra* note 3.

ss host w14p0.0000 .0000 cm0.00 0.00ang

ctexts –such ajeonnmobilthr victso

[66] Specifically, one commenter noted that, where data about a consumer's online activities is collected through the ISP rather than from individual websites that the consumer visits (*see* discussion *supra* note 40), the company collecting the data does not have a direct relationship with the websites. Therefore, the company is not in a position to require the sites to provide consumers with notice and choice about data collection and use for behavioral advertising. Consequently, this commenter suggested that the Principles should contemplate notice and choice mechanisms outside the website context.

[67] *See, e.g.*, Jon Leibowitz, Commissioner, FTC, Remarks at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting, & Technology" at 4-5 (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf;

available at http://www.ftc.gov/os/2007/06/P025505MortgageDisclosureReport.pdf; Kleimann Comm. Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Projec1y*

information about consumers' online activities. Staff commends such efforts.

D. Affirmative Express Consent for Material Retroactive Changes to Privacy Promises

Many commenters discussed the material change principle, which calls upon companies to obtain affirmative express consent before they use data in a manner that is materially different from the promises the company made at the time of collection. A number of industry commenters objected to this principle as proposed. These commenters called for more flexibility so that companies, in determining the type of notice and choice to offer consumers, can take into account the type of data affected and its sensitivity. The commenters argued that requiring notice and opt-in choice for material changes with respect to all types of data is not only unnecessary, but also is technologically unworkable, and could cause consumer confusion and inconvenience. Additionally, several of these comm

immaterial to consumers and may not warrant the costs and burdens of obtaining consumers’

[73] Under Commission law and policy, the term “material” refers to whether a practice, or information about a practice, is likely to affect a consumer’s conduct or decisions with regard to a product or service. *See* FTC Policy Statement on Deception, *supra* note 70, at Part IV. Similarly, a “material change” refers to a change in a company’s practices that, if known to the consumer, would likely affect the consumer’s conduct or decisions with respect to the company’s products or services.

[74] Many companies provide some form of prominent notice and opt-out choice for prospective changes – by sending an email notice to their customers, for example, or providing a prominent notice on the landing page of their website. Depending on the circumstances, such an approach may be sufficient. Of course, in deciding how to address prospective material changes, companies must consider such factors as: what claims were made in the original privacy policy, the sensitivity of the information at issue, and the need to ensure that any repeat visitors to a website are sufficiently alerted to the change.

tser To D7200 0.0’.

changes only.

E. Affirmative Express Consent to (or Prohibition Against) Use of Sensitive Data

The fourth principle states that companies should only collect sensitive data for behavioral advertising after they obtain affirmative express consent from the consumer t

[75] The sensitivity of precise geographic location information was also discussed at a panel on mobile "location-based services" during the FTC's 2008 Town Hall on mobile marketing. *See* Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace* (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

These commenters specifically cited the COPPA Rule (children'

warranted.[77] Indeed, this protection is particularly important in the context of online behavioral advertising, where data collection is typically invisible to consumers who may believe that they are searching anonymously for information about medications, diseases, sexual orientation, or other highly sensitive topics. Moreover, contrary to the suggestions in the comments, existing statutory regimes do not address most types of online behavioral advertising or the privacy concerns that such advertising raises.

With respect to defining what constitutes sensitive data, staff agrees with the commenters that such a task is complex and may often depend on the context. Although financial data, data about children, health information, precise geographic location information, and Social Security numbers are the cleare

[77] As discussed previously, *supra* note 70, pre-checked boxes or disclosures that are buried in a privacy policy or a uniform licensing agreement are unlikely to be sufficiently prominent to obtain a consumer's "affirmative express consent."

and some consumer groups cited potential harmful secondary uses, including selling personally identifiable behavioral data, linking click stream data to PII from other sources, or using behavioral data to make credit or insurance decisions. These commenters noted, however, that such uses do not appear to be well-documented. Some commenters recommended that the FTC seek more information regarding secondary uses, including the extent to which the collection of data by third-party applications operating on a host website constitutes secondary use.

Given the dearth of responses to staff's request for specific information, it is unclear whether companies currently use tracking data for non-behavioral advertising purposes other than the internal operations identified above.[78] Staff therefore does not propose to address this issue in the Principles at this time. Staff agrees with some of the commenters, however, that the issue of secondary use merits additional consideration and dialogue. Therefore, as staff

s staff54 TD(n thnci1les at this tim)18.3600 0.0000 TDm0.0 TD(continu TDm0.(IV)'taff)0 0.0000 TD(bo)ff

[78] Where companies are using tracking data for non-behavioral advertising purposes, such uses may involve sharing the data with third parties. If so, the notice and choice that a company provides concerning such sharing may address at least some of the concerns raised about secondary uses. A secondary use may also constitute a retroactive "material change" to a company's existing privacy policy, in which case consumers could choose whether to provide affirmative express consent to the change.

applicable federal and state laws.

---

nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company. ***Companies should also retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.***

ƨ ƨ ɹ

Looking forward, the Commission will continue to