FTC Staff Report:

Self-Regulatory Principles For Online Behavioral Advertising

February 2009

TABLE OF CONTENTS

EXECUTIVE SUMMARY. i

I. INTRODUCTION. 1

II. BACKGROUND. 2
- A. What Is Online Behavioral Advertising?. 2
- B. The FTC's Examination of Online Behavioral Advertising. 4
  - 1. Online Profiling Workshop. 6
  - 2. Tech-ade Hearings and the Ehavioral Advertising Town Hall. 8
- C. Staff's Proposed Self-Regulatory Principles. 11
- D. Recent Initiatives to Address Privacy Concerns. 12

III. SUMMARY OF THE COMMENTS RECEIVED AND STAFF'S ANALYSIS. 18
- A. The Principles' Scope. 20
  - 1. Applicability to Non-PII. 20
  - 2. Applicability to "First Party" Online Behavioral Advertising. 26
  - 3. Applicability to Contextual Advertising. 29
- B. Transparency and Consumer Control.. 30
  - 1. Choice for Non-PII.. 31
  - 2. Providing Effective Notice and Choice. 33
- C. Reasonable Security and Limited Data Retention for Consumer Data. 37
- D. Affirmative Express Consent for Material Retroactive Changes to Privacy Promises.. 39
- E. Affirmative Express Consent to (or Prohibition Against) Use of Sensitive Data 42
- F. Secondary Uses.. 44

IV. REVISED PRINCIPLES. 45
- A. Definition. 46
- B. Principles. 46
  - 1. Transparency and Consumer Control.. 46
  - 2. Reasonable Security, and Limited Data Retention, for Consumer Data. 46
  - 3. Affirmative Express Consent for Material Changes to Existing Privacy Promises.. 47
  - 4. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising. 47

V. CONCLUSION. 47

FTC STAFF REPORT:
SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING

EXECUTIVE SUMMARY

Since the emergence of "e-commerce" in the mid-1990s, the online marketplace has continued to expand and evolve, creating new business models that allow greater interactivity between consumers and online companies. This expanding marketplace has provided many benefits to consumers, including free access to rich sources of information and the convenience of shopping for goods and services from home. At the same time, the ease with which companies can collect and combine information from consumers online has raised questions and concerns about consumer privacy.

Starting in 1995, the Federal Trade Commission ("FTC" or "Commission") has sought to understand the online marketplace and the privacy issues it raises for consumers. The Commission has hosted numerous public workshops and has issued public reports focusing on online data collection practices, industry self-regulatory efforts, and technological developments affecting consumer privacy. As part of this effort, the Commission has examined online behavioral advertising – the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests. In November 2007, the FTC held a two-day "Town Hall," which brought together numerous interested parties to discuss online behavioral advertising in a public forum.

Participants at the Town Hall discussed the potential benefits of the practice to consumers, including the free online content that online advertising generally supports, the personalized advertising that many consumers may value, and a potential reduction in unwanted advertising. They also discussed the privacy concerns that the practice raises, including the

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. Staff also attempted to balance the potential benefits of behavioral advertising against the privacy concerns. Specifically, the Principles provide for transparency and consumer control and reasonable security for consumer data. They also call for companies to obtain affirmative express consent from consumers before they use data in a manner that is materially different than promised at the time of collection and before they collect and use "sensitive" consumer data for behavioral advertising. In addition to proposing the Principles, staff also requested information concerning the use of tracking data for purposes unrelated to behavioral advertising.

Staff received sixty-three comments on the Principles from eighty-seven stakeholders, including individual companies, business groups, academics, consumer and privacy advocates, and individual consumers. Many commenters addressed the Principles' scope, an issue that cuts across each of the individual principles. In particular, commenters discussed whether the Principles should apply to practices involving information that is not personally identifiable and whether they should apply to "first party" and "contextual" behavioral advertising models. As discussed further in this Report, staff believes that the Principles should apply to data that could

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 between personally identifiable and non-personally identifiable information increasingly unclear. Moreover, this approach is consistent with existing self-regulatory efforts in this area.

Staff agrees with some of the commenters, however, that the Principles' scope could be more narrowly focused in two important respects. First, it appears that "first party" behavioral advertising – behavioral advertising by and at a single website – is more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than other forms of behavioral advertising. Second, staff believes that contextual advertising – advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result – is likely to be less invasive than other forms of behavioral advertising. Accordingly, staff believes that the Principles need not cover these practices. Staff notes, however, that some of the Principles are based on existing Commission law and policy. Therefore, regardless of the scope of the Principles, companies must still comply with existing legal obligations to provide reasonable security for consumer data. Further, companies must adhere to the promises they make regarding how they collect, use, store, and disclose data, and cannot make unilateral, "material changes" to such promises without consumers' consent.

In addition to addressing the Principles' overall scope, numerous commenters discussed the individual principles. In particular, commenters discussed whether and how to provide transparency and consumer choice for online behavioral advertising. They also raised issues related to the material change principle and questioned how to define "sensitive" data and the

appropriate protections for such data. Relatively few of the commenters answered staff's request for additional information on other uses for tracking data. This Report discusses the main points addressed in the comments, provides further guidance regarding the scope and application of the Principles, and sets forth revised Principles. It also discusses recent initiatives by industry, consumer groups, and others to address the consumer privacy concerns raised by online behavioral advertising.

This Report constitutes the next step in an ongoing process to examine behavioral advertising that involves the FTC, industry, consumer and privacy organizations, and individual consumers. Although the comments have helped to frame the policy issues and inform public understanding of online behavioral advertising, the practices continue to evolve and significant work remains. Some companies and industry groups have begun to develop new privacy policies and self-regulatory approaches, but more needs to be done to educate consumers about online behavioral advertising and provide effective protections for consumers' privacy. Staff, therefore, will continue to examine this marketplace and take actions to protect consumers as appropriate.

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 behavioral advertising – the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests.[1] Staff developed these principles (the "Principles") based on an ongoing examination of the consumer issues raised by behavioral advertising and the public discussion of these issues at the FTC's November 2007 "Ehavioral Advertising" Town Hall.[2] Staff's goals in releasing the Principles were to spur continuing public dialogue about the issues and to encourage industry to develop meaningful self-regulation in this area.

In developing the proposed Principles, staff attempted to balance the privacy concerns raised by online behavioral advertising against the potential benefits of the practice. Consumers have genuine and legitimate concerns about how their data is collected, stored, and used online. They may also benefit, however, from the free content that online advertising generally supports, as well as the personalization of advertising that many consumers appear to value. Thus, any self-regulatory program in this area should address practices that raise genuine privacy concerns without interfering with practices – or stifling innovation – where privacy concerns are minimal.

In response to the proposed Principles, staff received over sixty comments from various stakeholders, including industry, privacy advocates, technologists, consumers, academics, and state and foreign governmental entities. The comments have helped to further staff's

---

[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.

understanding of the complex and rapidly evolving online behavioral advertising marketplace. At the same time, the comments raised additional issues and questions for consideration, and many of them called upon Commission staff to provide more guidance. This Report summarizes and responds to the main issues raised in the comments. In addition, the Report provides guidance on the Principles and sets forth revised principles consistent with this guidance.

II. BACKGROUND

A. What Is Online Behavioral Advertising?

Online behavioral advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience. In many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar identifier that could be used to identify the consumer in the offline world. Instead, businesses generally use "cookies"[3] to track consumers' activities and associate those activities with a particular computer or device.[4] Many of the companies engaged in behavioral advertising are so-called

[3] A cookie is a small text file that a website's server places on a computer's web browser. The cookie transmits information back to the website's server about the browsing activities of the computer user on the site. This includes information such as pages and content viewed, the time and duration of visits, search queries entered into search engines, and whether a computer user clicked on an advertisement. Cookies also can be used to maintain data related to a particular individual, including passwords or items in an online shopping cart. In some contexts, such as where a number of separate websites participate in a network, cookies can be used to track a computer user across different sites. In addition to cookies, there are other devices for tracking online activities, including "web bugs," "web beacons," and "Flash cookies."

[4] As discussed below, however, it may be possible to link or merge the collected information with personally identifiable information – for example, name, address, and other information provided by a consumer when the consumer registers at a website.

"network advertisers," companies that select and deliver advertisements across the Internet at websites that participate in their networks.[5]

An example of how behavioral advertising might work is as follows: a consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights from Washington D.C. to New York City.

In this simple example, the travel website where the consumer conducted his research might have an arrangement with a network advertiser to provide advertising to its visitors. The network advertiser places on the consumer's computer a cookie, which is tied to non-personally identifiable information such as the web pages the consumer has visited, the advertisements that the consumer has been shown, and how frequently each advertisement has been shown. Because the newspaper's website is also part of the advertising network, when the consumer visits the newspaper website the network advertiser's cookie identifies the consumer as a visitor to the travel website who likely has an interest in traveling to New York. It then serves the corresponding advertisement for airline flights to New York.

In a slightly more sophisticated example, the information about the consumer's activities on the travel website could be combined with information about the content that the consumer viewed on the newspaper's website. The advertisement served could then be tailored to the consumer's interest in, not just New York City, but also baseball (*e.g.*, an advertisement

[5] Ads from network advertisers are usually delivered based upon data collected about a given consumer as he or she travels across the different websites in the advertising network. An individual network may include hundreds or thousands of different, unrelated websites and an individual website may belong to multiple networks.

referring to the New York Yankees).

B. The FTC's Examination of Online Behavioral Advertising

The Federal Trade Commission's involvement with online privacy issues, including behavioral advertising, dates back to the emergence of "e-commerce."[6] Since that time, the Commission has sought to understand the marketplace, to evaluate the costs and benefits of various practices affecting consumers, and to stop unfair or deceptive practices. At the same time, given the dynamic nature of this marketplace and the technologies that make it possible, the Commission has consistently sought to avoid stifling innovation so that responsible business practices could develop and flourish. The Commission has engaged in a continuous dialogue with members of industry, consumer and privacy advocates, technology experts, consumers, and other interested parties. Starting in 1995, the Commission has conducted a series of public workshops and has issued reports focusing on online data collection practices, industry's self-regulatory efforts, and technological efforts to enhance consumer privacy.[7] In addition to these

---

[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 described the Commission's involvement in online privacy issues and recommended that Congress enact online privacy legislation based upon "fair information practice" principles for consumer-oriented commercial websites.

[7] *See, e.g.*, FTC Town Hall, *Beyond Voice: Mapping the Mobile Marketplace* (May 6-7, 2008), *available at* http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml; FTC Workshop, *Protecting Personal Information: Best Practices for Business* (Apr. 15, 2008, Aug. 13, 2008, and Nov. 13, 2008), *available at* http://www.ftc.gov/bcp/workshops/infosecurity/index.shtml; FTC Workshop, *Security in Numbers: SSNs and ID Theft* (Dec. 10-11, 2007), *available at* http://www.ftc.gov/bcp/workshops/ssn/index.shtml; FTC Staff Report, *Spam Summit: The Next Generation of Threats and Solutions* (Nov. 2007), *available at* http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf; FTC Summit, *Spam Summit: The Next Generation of Threats and Solutions* (July 11-12, 2007), *available at* http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml; FTC Staff Report, *Radio*

policy initiatives, the Commission and its staff have conducted investigations and brought law enforcement actions challenging such practices as deceptive privacy claims and improper disclosure of consumer data.[8]

Frequency IDentification: Applications and Implications for Consumers (Mar. 2005), *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf; FTC Workshop, *Radio Frequency IDentification: Applications and Implications for Consumers* (June 21, 2004), *available at* http://www.ftc.gov/bcp/workshops/rfid/index.shtm; FTC Workshop, *Monitoring Software on Your PC: Spyware, Adware and Other Software* (Apr. 19, 2004), *available at* http://www.ftc.gov/bcp/workshops/spyware/index.shtm; FTC Forum, *Spam Forum* (Apr. 30-May 2, 2003), *available at* http://www.ftc.gov/bcp/workshops/spam/index.shtml; FTC Workshop, *Consumer Information Security Workshop* (May 20-21, 2002), *available at* http://www.ftc.gov/bcp/workshops/security/index.shtm; FTC Report, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues* (Feb. 2002), *available at* http://www.ftc.gov/bcp/reports/wirelesssummary.pdf; FTC Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 2001), *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues* (Dec. 11-12, 2000), *available at* http://www.ftc.gov/bcp/workshops/wireless/index.shtml; FTC Report, *Consumer Protection in the Global Electronic Marketplace: Looking Ahead* (Sept. 2000), *available at* http://www.ftc.gov/bcp/icpw/lookingahead/electronicmkpl.pdf; FTC Workshop, *U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace* (June 1999), *available at* http://www.ftc.gov/bcp/icpw/lookingahead/global.shtm; FTC Staff Report*, Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996), *available at* http://www.ftc.gov/reports/privacy/privacy.pdf; FTC Workshop, *Consumer Privacy on the Global Information Infrastructure* (June 1996), *available at* http://www.ftc.gov/bcp/privacy/wkshp96/privacy.shtm.

[8] Since 2001, the Commission has brought twenty-three actions against companies that allegedly failed to provide reasonable protections for sensitive consumer information in both online and offline settings. *See FTC v. Navone*, No. 2:08-CV-01842 (D. Nev. filed Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Genica Corp.*, FTC Matter No. 082-3133 (Feb. 5, 2009) (proposed consent agreement); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC

1. Online Profiling Workshop

As a part of these efforts, in November 1999 the FTC and the Department of Commerce jointly sponsored a public workshop to examine the privacy implications of "online profiling" – essentially, an early form of online behavioral advertising.[9] Based upon the workshop, the FTC prepared two reports to Congress. The first, *Online Profiling: A Report to Congress* (June 2000) ("June 2000 Report"), described how online profiling operates and addressed the concerns that many of the workshop participants raised about the collection of detailed consumer data and the practice's lack of transparency.[10] The June 2000 Report also described online profiling's potential benefits to consumers, as well as to businesses. These benefits included delivering more relevant ads to consumers, subsidizing free online content, and allowing businesses to market more precisely and spend their advertising dollars more effectively.

The Commission's second report, *Online Profiling: A Report to Congress Part 2*

Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[9] FTC and Department of Commerce Workshop, *Online Profiling Public Workshop* (Nov. 8, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/index.shtm.

[10] June 2000 Report, *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf. The June 2000 Report stated that "[m]any commenters at the Workshop objected to networks' hidden monitoring of consumers and collection of extensive personal data without consumers' knowledge or consent; they also noted that network advertisers offer consumers few, if any, choices about the use and dissemination of their individual information obtained in this manner." *Id.* at 10.

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") in response to concerns raised at the 1999 workshop and submitted them to the FTC and the Department of Commerce for consideration. In the July 2000 Report, the Commission commended the NAI companies' efforts in developing principles that included various protections to govern the collection and use of consumer data online.[12] Nevertheless, while acknowledging that "self-regulation is an important and powerful mechanism for protecting consumers," a majority of the Commission recommended that Congress enact "backstop legislation" to address online profiling.[13]

Ultimately, Congress did not enact legislation to address online profiling. In the meantime, with the "burst" of the dot-com bubble, the number of network advertisers declined dramatically such that by the early 2000s, many had gone out of business.[14]

---

[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).

2. Tech-ade Hearings and the Ehavioral Advertising Town Hall

By the middle of the decade, the online advertising market, including the behavioral advertising market, had regained its footing. Indeed, online advertising spending grew dramatically between 2002 and 2006, with estimated sales rising from $6 billion to over $16.6 billion.[15] These changes in the marketplace, and the growing practice of behavioral advertising, were a featured topic at the FTC's November 2006 "Tech-ade" hearings,[16] which examined the consumer protection challenges anticipated over the next ten years. Participants at the hearings described how technological advances had allowed for greater and more efficient use of online profiling (now called "behavioral" advertising, targeting, or marketing) and brought renewed attention to the practice.[17]

In the months after the Tech-ade hearings, staff launched an effort to learn more about online behavioral advertising. At the same time, several organizations petitioned the Commission to reexamine the privacy issues raised by the practice.[18] Further, the announcement

---

[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/transcripts.html.

[17] *See* Transcript of Hearing Record at 46-107, *Protecting Consumers in the Next Tech-ade* (Nov. 7, 2006), *available at* http://www.ftc.gov/bcp/workshops/techade/pdfs/transcript_061107.pdf (panel discussion entitled "Marketing and Advertising in the Next Tech-ade").

[18] *See, e.g.*, Letter from Ari Schwartz, Executive Director, and Alissa Cooper, Policy Analyst, Center for Democracy and Technology ("CDT"), to J. Thomas Rosch, Commissioner, FTC (Jan. 19, 2007), *available at* http://www.cdt.org/privacy/20070119rosch-behavioral-letter.pdf; Center for Digital Democracy ("CDD") and U.S. Public Interest Research Group, Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov. 1, 2006), *available at* http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf.

of the proposed merger between Google, Inc. ("Google") and DoubleClick, Inc. in April 2007 raised concerns about the combination of large databases of consumer information and the potential development of detailed consumer profiles.[19] Commission staff met with dozens of industry representatives, technology experts, consumer and privacy advocates, and academics. These meetings aided staff's understanding of the changes to the industry since the 1999 workshop and allowed staff to identify key questions and issues for further discussion.

In November 2007, the FTC held its "Ehavioral Advertising Town Hall," a two-day public meeting that brought together various interested parties to discuss the privacy issues surrounding online behavioral advertising.[20] Based on the discussion, several core principles emerged. First, as discussed above, online behavioral advertising[21] may provide valuable

---

[19] *See* Letter from Jeffrey Chester, Executive Director, CDD, to Deborah Platt Majoras, Chairman, FTC et al. (Dec. 10, 2007), *available at* http://www.democraticmedia.org/files/FTCletter121007.pdf; Letter from Mindy Bockstein, Executive Director, New York State Consumer Protection Board, to Deborah Platt Majoras, Chairman, FTC, Re: DoubleClick Inc. and Google, Inc. Merger (May 1, 2007), *available at* http://epic.org/privacy/ftc/google/cpb.pdf. The Commission approved the merger on December 20, 2007, at the same time that it issued the Principles. *See Statement of Federal Trade Commission Concerning Google/DoubleClick*, FTC File No. 071-0170 (Dec. 20, 2007), *available at* http://www.ftc.gov/os/caselist/0710170/071220statement.pdf.

[20] The complete transcripts of the Town Hall entitled *Ehavioral Advertising: Tracking, Targeting & Technology* are available at http://www.ftc.gov/bcp/workshops/ehavioral/71101wor.pdf and http://www.ftc.gov/bcp/workshops/ehavioral/71102wor.pdf.

[21] To facilitate a comprehensive discussion of the issues at the Ehavioral Advertising Town Hall, the FTC applied a broad definition of online behavioral advertising – namely, the collection of information about a consumer's online activities in order to deliver advertising targeted to the individual consumer's interests. This definition was meant to encompass the various tracking activities engaged in by diverse companies across the web. *See* Transcript of Town Hall Record at 8, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/71101wor.pdf (introductory remarks of Lydia B. Parnes, Director, FTC Bureau of Consumer Protection) [hereinafter "Nov. 1 Transcript"]. FTC staff used a similar definition in its proposed Principles.

benefits to consumers in the form of free content, personalization that many consumers appear to value, and a potential reduction in unwanted advertising. Second, the invisibility of the practice to consumers raises privacy concerns, as does the risk that data collected for behavioral advertising – including sensitive data about children, health, or finances – could be misused. Third, business and consumer groups alike expressed support for transparency and consumer control in the online marketplace.[22]

A number of Town Hall participants also criticized existing self-regulatory efforts. Specifically, these participants stated that the NAI Principles had not been effective to address the privacy concerns that online behavioral advertising raises. They argued that the NAI Principles were too limited because they applied only to network advertisers and not to other business models. Other critics cited the purported lack of enforcement of the NAI Principles and its cumbersome and inaccessible opt-out system.[23] Further, while various industry associations discussed their online self-regulatory schemes to address privacy issues, these schemes did not generally focus on behavioral advertising.[24]

---

[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"].

[24] *Id.* at 135-143, 155-159. As an alternative to the existing self-regulatory models, and in an effort to increase consumers' control over the tracking of their online activities, a coalition of privacy groups proposed the development of a "Do Not Track List." *See* Ari Schwartz, CDT,

C. Staff's Proposed Self-Regulatory Principles

In response to the issues raised at the Town Hall, and to continue the dialogue with interested parties, in December 2007 Commission staff released the proposed self-regulatory Principles for public comment. Staff supported self-regulation because it provides the necessary flexibility to address evolving online business models. At the same time, however, staff recognized that existing self-regulatory efforts had not provided comprehensive and accessible protections to consumers. Accordingly, in issuing the proposed Principles, staff intended to guide industry in developing more meaningful and effective self-regulatory models than had been developed to date.

The proposed Principles include four governing concepts. The first is transparency and control: companies that collect information for behavioral advertising should provide meaningful disclosures to consumers about the practice and choice about whether to allow the practice. The second principle proposes reasonable security and limited data retention: companies should provide reasonable data security measures so that behavioral data does not fall into the wrong hands, and should retain data only as long as necessary for legitimate business or law enforcement needs. The third principle governs material changes to privacy policies: before a company uses behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the

---

et al., *Consumer Rights and Protections in the Behavioral Advertising Sector*, *available at* http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf (Oct. 31, 2007) (the proposed "Do Not Track List" is modeled after the FTC's national "Do Not Call" registry and would require online advertisers using a persistent identifier to provide to the FTC the domain names of the servers or other devices placing the identifier).

consumer.[25] The fourth principle states that companies should obtain affirmative express consent before they use sensitive data – for example, data about children, health, or finances – for behavioral advertising.[26] Finally, staff's proposal requested additional information regarding the potential uses of tracking data other than for behavioral advertising, including whether such secondary uses raise concerns and merit heightened protection.

D. Recent Initiatives to Address Privacy Concerns

Following the Town Hall and the release of the Principles, various individual companies, industry organizations, and privacy groups have taken steps to address some of the concerns and issues raised by online behavioral advertising. For example, a number of companies have developed new policies and procedures to inform consumers about online tracking and provide additional protections and controls over the practice.[27] In particular, both Google and Yahoo! Inc. ("Yahoo!") have announced new tools that will allow consumers to opt out of receiving targeted online advertisements.[28] Microsoft Corporation has announced that the new version of

---

[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 (alleging that the company made material changes to its privacy policy and applied such changes to data collected under the old policy). The FTC's order requires Gateway to obtain opt-in consent for such changes in the future.

[26] Staff recommended that companies obtain consumers' affirmative express consent for material, retroactive changes and for the use of sensitive data because of the increased privacy concerns raised by the collection and use of such data.

[27] FTC staff encourages continued stakeholder efforts to address the privacy concerns raised by behavioral advertising, but does not endorse any of the specific approaches described herein.

[28] *See* Press Release, Yahoo!, *Yahoo! Announces New Privacy Choice for Consumers* (Aug. 8, 2008), *available at* http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=327212; Posting of Rajas Moonka, Senior Business Product Manager, Google, to

its Internet browser will include a tool that, when enabled by a user, will not save browsing and searching history, cookies, form data, or passwords, and will automatically clear the browser cache at the end of each session.[29] Other steps include educational programs to inform consumers about online tracking[30] and new policies to reduce the length of time companies store personal data collected about online searches.[31]

In December 2008, in response to the criticism of the NAI Principles at the Town Hall and the FTC's call for stronger self-regulation, the NAI issued revised principles ("NAI 2008 Principles").[32] Although NAI has strengthened certain aspects of its self-regulatory regime –

---

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); YouTube, Google Search Privacy Playlist, http://www.youtube.com/view_play_list?p=ECB20E29232BCBBA (last visited Jan. 9, 2009).

[31] *See* Posting of Kim Hart, washingtonpost.com, to http://voices.washingtonpost.com/posttech/2008/12/yahoo_changes_data-retention_p.html?nav=rss_blog (Dec. 17, 2008, 13:50 EST) (stating that Yahoo! agreed to shorten online behavioral data retention periods from thirteen to three months); Posting of Stacey Higginbotham, GigaOM, to http://gigaom.com/2008/09/09/in-online-privacy-fight-google-blinks/ (Sept. 9, 2008, 7:47 PT) (stating that Google agreed to reduce storage of search engine inquiries from eighteen to nine months); *see also Microsoft to Cut Search Engine Data Retention to Six Months if Others Follow*, 7 PRIVACY & SEC. LAW REP. 1767 (2008) (stating that Microsoft announced it would reduce search engine data retention to six months in the European Union if all search companies agreed to do the same).

[32] *See* NAI, *2008 NAI Principles Code of Conduct* (Dec. 16, 2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf [hereinafter "NAI 2008 Principles"]. In advance of issuing the NAI 2008 Principles,

most notably by dramatically increasing its membership – staff believes that NAI could do more to ensure the transparency of online behavioral advertising to consumers. Staff also notes that certain elements of NAI's revised approach have yet to be clarified through implementation guidelines, which NAI plans to issue in 2009.[33] More recently, a joint industry task force including marketing and industry trade associations, as well as the Council of Better Business Bureaus, announced a cooperative effort to develop self-regulatory principles to address privacy concerns related to online behavioral advertising.[34]

NAI issued proposed principles for public comment in April 2008. *See* NAI, *Draft 2008 NAI Principles* (Apr. 10, 2008), *available at* http://www.networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf. In some respects, NAI's proposed principles contained stronger protections than those announced in December. For example, NAI's original proposal prohibited the use of certain categories of sensitive information, including information about children, for behavioral advertising. As finalized, the NAI 2008 Principles would allow use of these categories of information so long as consumers (or parents, in the case of children) provide their consent.

[33] The NAI 2008 Principles expand the security and access requirements to cover data used for behavioral advertising, as well as data used for practices such as tracking the number of ads served at a particular website. They also restrict NAI members' use of behavioral advertising data to marketing purposes and require that members retain such data only as long as needed for legitimate business purposes or as required by law. FTC staff commends NAI's attempts to strengthen its principles through these and other steps. At the same time, staff notes that there are areas where NAI may continue to improve. For example, staff notes that the NAI 2008 Principles' approach to providing notice and choice generally mirrors NAI's previous approach – *i.e.*, members may continue to provide notice to consumers through website privacy policies. For the reasons discussed below, staff encourages companies engaged in online behavioral advertising to develop mechanisms that allow for prominent disclosure outside companies' existing privacy policies. Moreover, because the revisions tie some obligations to certain language (*e.g.*, "directly engaging" in behavioral advertising) that will be defined through future implementation guidelines, the impact of these obligations is currently unclear. Similarly, because NAI plans to issue further guidance regarding the policies and procedures governing its compliance reviews, questions remain as to whether these reviews, and any penalties that are ultimately imposed, will be adequate to ensure compliance.

[34] The initiative includes the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, and the Interactive Advertising Bureau ("IAB"). *See* K.C. Jones, *Agencies to Self-Regulate Online Behavioral Ads*,

Several other organizations have also developed materials to assist online businesses in identifying and addressing privacy concerns raised by online behavioral advertising. For example, the Future of Privacy Forum – an advocacy group of privacy scholars, lawyers, and corporate officials – has launched an initiative to develop new ways to provide consumers with control over the use of their personal information for online behavioral advertising.[35] The Center for Democracy and Technology ("CDT") also recently released an assessment tool, developed in conjunction with internet companies and public interest advocates, to help online companies evaluate the consumer privacy implications of their online behavioral advertising practices and to create appropriate, meaningful privacy protections.[36] Finally, TRUSTe, a privacy seal organization, has issued a white paper reviewing the current online behavioral advertising environment and providing a checklist to assist online companies to address issues raised by online behavioral advertising, especially those concerning transparency.[37]

Congress has also expressed concern about the privacy issues raised by online behavioral

---

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 that its member companies notify consumers about data collection practices and provide choice when appropriate. IAB, *Privacy Principles* (Feb. 24, 2008), *available at* http://www.iab.net/iab_products_and_industry_services/1421/1443/1464.

[35] *See* Kim Hart, *A New Voice in Online Privacy*, WASH. POST, Nov. 17, 2008, at A06, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/11/16/AR2008111601624.html?nav=hcmoduletmv.

[36] *See* CDT, *Threshold Analysis for Online Advertising Practices* (Jan. 2009), *available at* http://www.cdt.org/privacy/20090128threshold.pdf.

[37] *See* TRUSTe, *Online Behavioral Advertising: A Checklist of Practices that Impact Consumer Trust*, *available at* http://www.truste.com/about/online_behavioral_advertising.php (last visited Feb. 3, 2009).

advertising. On July 9, 2008, the Senate Committee on Commerce, Science, and Transportation ("Senate Committee") held a hearing entitled "Privacy Implications of Online Advertising," which examined the online advertising industry and the impact of these practices on consumers' privacy.[38] Witnesses from the FTC,[39] consumer groups, and industry discussed both the methods of online behavioral advertising employed by industry and the government's role in protecting consumer privacy. The Senate Committee held a follow-up hearing on September 25, 2008, which focused on behavioral advertising in conjunction with Internet Service Providers ("ISPs").[40] Testifying at the second hearing, corporate officers representing Verizon Communications, Inc., AT&T Services, Inc., and Time Warner Cable expressed support for self-regulation by the various entities engaged in online behavioral advertising practices. Specifically, these representatives called for a requirement that companies obtain opt-in consent from consumers before collecting online information for behavioral advertising purposes.

---

[38] *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 110th Cong. (2008), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf37017.

[39] *See id.* (statement of Lydia Parnes, Director of the FTC Bureau of Consumer Protection).

[40] *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 110th Cong. (2008), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=778594fe-a171-4906-a585-15f19e2d602a. In the ISP-based behavioral advertising model, a consumer's online activities are collected directly from the consumer's ISP, rather than from the individual websites the consumer visits. This model, which is also often referred to as "deep packet inspection," could potentially allow targeting of ads based on substantially all of the websites a consumer visits, rather than simply a consumer's visits to, and activities within, a given network of websites. *See* Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 4, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html.

The House Committee on Energy and Commerce ("House Committee"), and its Subcommittee on Telecommunications and the Internet ("Telecommunications Subcommittee"), also have been active in this area, focusing in particular on ISP-related practices. On July 17, 2008, the Telecommunications Subcommittee held a hearing entitled "What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies" that included testimony from industry, experts, and consumer groups.[41] Thereafter, on August 1, 2008, four members of the House Committee issued letters to thirty-four companies seeking information on their practices with respect to behavioral advertising.[42] The companies' responses are available online.[43]

These developments suggest that there is continuing public interest in the issues that behavioral advertising raises and increasing engagement by industry members in developing solutions.

---

[41] *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the H. Subcomm. on Telecomm. & the Internet*, 110th Cong. (2008), *available at* http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml.

[42] Letter from John D. Dingell, Chairman of the H. Comm. on Energy & Commerce, et al., to William Bresnan, Chairman & C.E.O. of Bresnan Communications, et al. (Aug. 1, 2008), *available at* http://energycommerce.house.gov/Press_110/110-ltr.080108.AOL-TILetters.pdf.

[43] H. Comm. on Energy & Commerce, Responses to Aug. 1, 2008 Letter to Network Operators Regarding Data Collection Practices, *available at* http://energycommerce.house.gov/Press_110/080108.ResponsesDataCollectionLetter.shtml (last visited Jan. 9, 2009). In light of concerns expressed by Congress and others, at least one high profile company suspended its plans to engage in ISP-based behavioral advertising. *See* Ellen Nakashima, *NebuAd Halts Plans For Web Tracking*, WASH. POST, Sept. 4, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html.

III. SUMMARY OF THE COMMENTS RECEIVED AND STAFF'S ANALYSIS

In response to the proposed Principles, FTC staff received sixty-three comments from interested parties; because some of the comments represent the views of multiple parties, a total number of approximately eighty-seven stakeholders participated in the comment process. FTC staff greatly appreciates the substantial work of the parties that submitted comments. The comments have helped to clarify the differing perspectives regarding how best to address the privacy issues that online behavioral advertising raises.

As a threshold matter, some commenters stated that FTC staff's call for self-regulation is unnecessary and that the Principles could interfere with a developing and rapidly changing marketplace.[44] Others concluded that the Principles do not go far enough and that sweeping legislation is necessary. Between these positions, a majority of the commenters expressed support for some form of self-regulation. Most commenters also identified certain aspects of the Principles that, in their view, raise important issues, merit more guidance, or should be changed.

Set forth below is a summary of the comments arranged by topic. This summary highlights and discusses the main points and positions represented by the comments as a whole. Also included are FTC staff's responses to these main points, along with additional guidance

---

[44] One trade association comment also suggested that self-regulation at the behest of a governmental entity such as the FTC cannot truly be self-regulatory. In addition, a newspaper association stated that applying the Principles to a newspaper's advertising-supported website would violate the First Amendment because it could affect the selection of content that is presented to the reader. In response, staff notes that the Commission has often called for, studied the effectiveness of, and made suggestions for improving self-regulatory schemes, and that such efforts do not implicate the First Amendment. *See, e.g.*, FTC Report, *Marketing Violent Entertainment to Children: A Fifth Follow-Up Review of Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries* 33 (Apr. 2007), *available at* http://www.ftc.gov/reports/violence/070412MarketingViolentEChildren.pdf; FTC Report, *Self-Regulation in the Alcohol Industry* 25 (June 2008), *available at* http://www.ftc.gov/os/2008/06/080626alcoholreport.pdf.

regarding the Principles. The key theme underlying this guidance is the need to balance the potential benefits of the various practices covered by the Principles against the privacy concerns the practices raise. Among other things, staff considered consumer expectations regarding the practices; the extent to which the practices are transparent; the potential for consumer harm; and the need to maintain vigorous competition in the online marketplace and avoid stifling innovation.

In providing this guidance, staff notes that nothing in the discussion is intended to preclude or discourage the implementation of responsible or "best" practices outside of the Principles. Staff also notes that some of the Principles closely parallel FTC law and policy, which continue to apply regardless of the scope or coverage of the Principles. For example, depending upon on the circumstances, a company whose practices fall outside the Principles may still be required to implement reasonable measures to address any privacy or security risks to consumers' information.[45] Similarly, regardless of the Principles, companies may not unilaterally alter their policies and use previously collected data in a manner that materially differs from the terms under which the data was originally collected.[46] Companies should also be mindful of the federal and state laws that may apply to their operations.

Finally, staff notes that the FTC's work in this area, including its commitment to engage the public on these issues, will continue beyond this Report. Although the comments provided considerable information about the various business models and policy issues surrounding

---

[45] *See supra* note 8 (citing FTC settlements requiring companies to implement reasonable information security programs to protect sensitive personal information).

[46] *See 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.

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 deceptive acts or practices in this area that would potentially violate Section 5 of the FTC Act.

A. The Principles' Scope

As proposed, the Principles apply broadly to companies engaged in online behavioral advertising, defined as tracking consumers' online activities in order to deliver advertising that is targeted to the individual consumers' interests. Numerous commenters addressed the Principles' scope – specifically, the Principles' applicability to different types of data and different advertising practices. These commenters emphasized three significant issues: the applicability of the Principles not only to the collection and use of personally identifiable information ("PII"), but also of non-personally identifiable information ("non-PII");[47] the applicability to "first party," or "intra-site," collection and use of data; and the applicability to online contextual advertising.

1. Applicability to Non-PII

A number of commenters, representing industry groups and individual companies, stated that because the Principles' definition of online behavioral advertising fails to distinguish

[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.

between PII and non-PII, the Principles apply too broadly. Claiming that there is little or no privacy interest in non-PII and a limited potential for harm, these commenters argued that the FTC should exclude such data from the Principles. The commenters also maintained that application of the Principles to non-PII would impose significant costs on business and could interfere with companies' ability to provide free online content to consumers.

Similarly, some commenters noted that non-PII has traditionally fallen outside the bounds of U.S. privacy laws and self-regulatory programs and that the Principles' inclusion of such data marks a departure from the Commission's current approach to privacy issues. Not all industry comments supported a bright line distinction between PII and non-PII, however. For instance, an individual company and a seal organization recommended that the Principles recognize a third category of data – *i.e.*, data that falls in between PII and non-PII. Another individual company noted that even information that is not considered personally identifying can raise privacy concerns.

In contrast to the majority of industry comments, a number of consumer and privacy groups expressed support for applying the Principles to data typically considered to be non-PII. Specifically, these commenters would apply the Principles to such data as Internet Protocol (IP) addresses,[48] cookie data, and other information that the commenters stated could allow a set of behaviors or actions to be associated with a particular individual or computer user, even if that individual is never identified by name.

Staff believes that, in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by

[48] An IP address is a numerical identifier assigned to a computer or device that connects to the Internet.

itself, determine the protections provided for consumer data. Indeed, in this context, the Commission and other stakeholders have long recognized that both PII and non-PII raise privacy issues,[49] a view that has gained even more currency in recent years for a number of reasons. First, depending on the way information is collected and stored, it may be possible to link or merge non-PII with PII. For example, a website might collect anonymous tracking data and then link that data with PII (*e.g.*, name, address) that the consumer provided when registering at the site. Second, with the development of new and more sophisticated technologies, it likely will become easier to identify an individual consumer based on information traditionally considered to be non-PII. For instance, although industry has traditionally considered most IP addresses to be non-PII, it soon may be possible to link more IP addresses to specific individuals.[50]

Third, even where certain items of information are anonymous by themselves, they can become identifiable when combined and linked by a common identifier. For example, a consumer's Internet activity might reveal the restaurants in the neighborhood where she eats, the stores at which she shops, the property values of houses recently sold on her block, and the

---

[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 dramatically increase the number of unique IP addresses. While improving connectivity, IPv6 will rely more heavily on static IP addresses, which can link an individual IP address to a particular device that is associated with a specific individual.

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 activities. Upon learning that the data had been posted online, these consumers expressed surprise and concern that the company stored data about their online activities – and stored it in a way that allowed the data to be associated, at least in some cases, with particular individuals.[53]

---

[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

In staff's view, the best approach is to include within the Principles' scope any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or with a particular computer or device. Whether information "reasonably could be associated" with a particular consumer or device will depend on the factual circumstances and available technologies, but would include, for example: clickstream data that, through reasonable efforts, could be combined with the consumer's website registration information; individual pieces of anonymous data combined into a profile sufficiently detailed that it could become identified with a particular person; and behavioral profiles that, while not associated with a particular consumer, are stored and used to deliver personalized advertising and content to a particular device.[54] Such an approach will ensure protections for consumer data that raises a consumer privacy interest without imposing undue costs where data is truly anonymous and privacy concerns are minimal. As noted above, this is also consistent with NAI's approach, the predominant industry self-regulatory model, which has mandated protections for both PII and

---

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, *Why "Anonymous" Data Sometimes Isn't*, WIRED, Dec. 13, 2007, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213 (describing University of Texas experiments with de-anonymized Netflix data); Latanya Sweeney, *Comments to the Department of Health and Human Services on "Standards of Privacy of Individually Identifiable Health Information"* (Apr. 26, 2002), *available at* http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.pdf (describing experiments on a state's anonymized cancer registry).

[54] As discussed below, staff has limited the scope of the Principles in several ways that also limit their application to data traditionally considered to be non-PII. *See* discussion *infra* Parts III.A.2 and 3.

non-PII since 2000.

2. Applicability to "First Party" Online Behavioral Advertising

The Principles' applicability to "first party," or "intra-site," online behavioral advertising also generated numerous comments, primarily from industry groups and individual companies. Most of these commenters objected to the Principles' application to behavioral advertising by, and at, a single website. Instead, they urged the Commission to limit the Principles to practices that involve the tracking of consumers' activities across different websites. These commenters argued that "first party" collection and use of consumer information is transparent and consistent with consumer expectations. Additionally, the commenters described a variety of services and operations, valued by consumers, that require "first party" data collection and use. These include product recommendations, tailored content, shopping cart services, website design and optimization, fraud detection, and security.

Some commenters, including an individual company and a seal organization, recognized that the tracking of consumers across multiple sites raises increased concern, but did not support excluding "first party" practices from self-regulation entirely. Other commenters, including an individual company and several consumer groups, generally supported the Principles' application to "first party" behavioral advertising.

After considering the comments, staff agrees that "first party" behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites. For example, under the "first party" model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (*e.g.*, "based on your interest in travel, you might enjoy the

following books"). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.

In addition, staff agrees that "first party" collection and use of consumer data may be necessary for a variety of consumer benefits and services. These include not only personalized content and other elements of the interactive online experience that consumers may value, but also important internal functions such as security measures, fraud prevention, and legal compliance.[55]

Finally, maintaining data for internal use only also limits the risk that the data will fall into the wrong hands. For that reason, privacy schemes in varied contexts have distinguished between a site's internal use of data and the sharing of data with third parties, imposing stronger

[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.

privacy protections for the latter.[56] Staff believes that the same distinction holds true here.

Based on these considerations, staff agrees that it is not necessary to include "first party" behavioral advertising practices within the scope of the Principles.[57] If a website collects and then sells or shares data with third parties for purposes of behavioral advertising,[58] or participates in a network that collects data at the site for purposes of behavioral advertising, however, such practices would remain within the scope of the Principles.[59]

---

[56] For instance, the Children's Online Privacy Protection Rule ("COPPA Rule") recognizes that sharing of children's personal information with third parties raises more concern than use of the information simply for internal purposes. For this reason the COPPA Rule requires that website operators obtain the highest level of verifiable parental consent where such information is shared and, where possible, that the website enable parents to choose whether to allow sharing. *See* 16 C.F.R. § 312.4 (2006); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,899 (Nov. 3, 1999), *available at* http://www.ftc.gov/os/1999/10/64fr59888.pdf. *See also* Direct Marketing Assocation ("DMA"), *Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary* (Jan. 2002), *available at* http://www.the-dma.org/guidelines/onlineguidelines.shtml (recommending choice when data is shared with third parties).

[57] Staff notes that some of the principles are based on existing Commission case law and policy. As such, a company engaged in first party practices may still be required to provide reasonable security for the consumer data it collects and maintains. Additionally, depending upon the specific circumstances, a company may be precluded from using previously collected data in a way that conflicts with the privacy promises in effect at the time the company collected the data.

[58] To the extent that websites share data with third-party service providers in order to deliver ads or perform some of the internal functions described above, such sharing will still be considered "first party" use, provided there is no further use of the data by the service provider.

[59] Several commenters argue that data collection and use within a family of websites – *e.g.*, sites under common ownership or control – should be considered "first party" for purposes of the Principles. The commenters stated that consumers will save costs due to partnering arrangements, that consumers expect and want the additional marketing opportunities created through data sharing among affiliated websites, and that the Gramm-Leach-Bliley Act (the "GLB Act") allows financial institutions to share data with affiliates.

Staff believes that whether data sharing among affiliated companies should be considered "first party," and thus outside the scope of the Principles, should turn on whether the relationship among the sites – and the possibility that they may share data – is sufficiently transparent and

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 is shown an advertisement for tennis rackets solely because he is visiting a tennis-focused website or has used a search engine to find stores that sell tennis rackets, the advertisement is contextual.

The commenters described contextual advertising as transparent and consistent with consumers' expectations, similar to the "first party" practices discussed above. They also stated that, rather than being surprised by the practice, consumers expect and want to receive an ad for a product or service when visiting a website that is related to that product or service. Additionally, a number of commenters noted that contextual advertising creates fewer risks to privacy because the practice does not rely on the collection of detailed information about the consumer's actions over time. One group of consumer and privacy advocates also stated that excluding contextual advertising from the Principles may provide companies with an incentive to store less data about consumers.

---

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).

In general, the comments described online contextual advertising as the delivery of ads based upon a consumer's current visit to a single web page or a single search query, without the collection and retention of data about the consumer's online activities over time. Based on this description, staff agrees that contextual advertising provides greater transparency than other forms of behavioral advertising, is more likely to be consistent with consumer expectations, and presents minimal privacy intrusion when weighed against the potential benefits to consumers. As discussed above, these benefits may include free content – made possible by the revenue from the sale of the advertisements – and receipt of contextually relevant ads that consumers may value. Staff consequently does not believe that it is necessary for the Principles to cover this form of online advertising.[60] It should be stressed that, based on the comments and other considerations, staff has defined contextual advertising narrowly. Where a practice involves the collection and retention of consumer data for future purposes beyond the immediate delivery of an ad or search result, the practice does not constitute contextual advertising.

B. Transparency and Consumer Control

Numerous commenters – including individual consumers, industry representatives, and consumer and privacy advocates – discussed the first proposed principle, which calls for greater transparency and consumer control of online behavioral advertising practices. Specifically, FTC staff proposed that websites where data is collected for behavioral advertising should provide prominent notice to consumers about such practices and should also offer consumers the ability to choose whether to allow such collection and use. In discussing this principle, commenters

[60] As discussed with respect to first party practices, companies engaged in online contextual advertising may still be subject to laws and policies that impose obligations outside of the Principles. *See supra* note 57.

focused primarily on two issues: whether to provide choice for the collection and use of non-PII, and how best to provide disclosures about the practices.

1. Choice for Non-PII

The commenters generally agreed that companies should notify consumers when they are collecting information about consumers' online activities for behavioral advertising. Indeed, several commenters noted that existing self-regulatory regimes currently require such notice.[61] Some industry trade groups and an individual company, however, stated that the first principle goes too far in proposing *choice* for the collection of non-PII. In general, these commenters made the same arguments with respect to choice for non-PII that are discussed above with respect to the overall scope of the Principles: that choice for non-PII is inconsistent with existing self-regulatory privacy schemes and laws; that there is a reduced privacy interest in, and risk of harm from, non-PII; and that choice will interfere with the free content and other benefits that online behavioral advertising offers. Some commenters also noted that consumers already have the ability to choose not to conduct business with websites that collect their data. These commenters suggested that consumers do not own the data that websites collect about them, and that there is no precedent for giving consumers the ability to dictate the terms upon which they use a website.[62]

---

[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 well as a number of individual consumers, supported the concept of choice for the collection and use of non-PII for behavioral advertising and several asserted that the principle should go even further. Some of these commenters called for an *opt-in* choice[63] before data is collected and recommended that consumers receive clear notice about the purpose for which their data is collected. A coalition of consumer groups described the principle as inadequate and recommended the "Do Not Track" registry to allow consumers to limit online tracking.[64] Individual consumers also submitted comments expressing support for notice and the ability to control whether to allow collection of information about their online activities. One consumer stated that companies should be required to obtain permission to collect data regardless of how they use it.

For the reasons discussed above with respect to the Principles' overall scope, FTC staff believes that companies should provide consumer choice for the collection of data for online behavioral advertising if the data reasonably could be associated with a particular consumer or with a particular computer or device. As noted, the line separating PII and non-PII has become increasingly indistinct, and the predominant industry self-regulatory program has already adopted an approach that protects both types of information. Available research also suggests

---

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' comments focused on the content of the disclosures and suggested that, in order for notice and consent to be effective, websites should not only disclose that information is collected, but should also specify the type of information collected, its uses, how long it will be retained, and with whom it will be shared. Other commenters – including an individual consumer and an online advertising company – suggested

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.

Another comment, filed by two academics, discussed the inherent problem with using cookies both to track consumers' online activities[65] and to record consumers' choice of whether to allow such tracking. These commenters noted that where consumers take steps to control the privacy of their online activities, through the use of anti-spyware software or by deleting cookies from their computer browsers, the consumers may unintentionally also block or delete the cookies that record their behavioral advertising preference. The commenters suggested possible solutions to this problem, including the development of standards for distinguishing between opt-out cookies and other types of cookies and modifying browser settings to give consumers greater control over their cookies.

Several companies also requested guidance regarding the form and content of notice in different contexts – such as on mobile devices, on "Web 2.0," and through ISPs – and questioned whether a uniform or standard approach can be created. For example, commenters raised questions regarding the mechanics of providing notice and choice in the Web 2.0 world, where a consumer may use several different third-party applications on a single, unrelated host web page. Some commenters raised issues regarding appropriate notice in the mobile context. Others

---

[65] *See supra* note 3.

stated that, as proposed, the transparency and control principle would exclude certain business models, including where an ISP collects, or allows a third party to collect, consumers' online data.[66] With respect to ISP-based behavioral advertising, these commenters recommended that the principle permit notice through direct communication from the ISP to its subscribers rather than on a website.

The differing perspectives on how best to provide consumers with effective notice and choice highlight the complexities surrounding this issue. Staff recognizes that it is now customary to include most privacy disclosures in a website's privacy policy. Unfortunately, as noted by many of the commenters and by many participants at the FTC's November 2007 Town Hall, privacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers.[67] Staff therefore encourages companies to design innovative ways – outside of the privacy policy – to provide behavioral advertising disclosures and choice options to consumers.

A number of the commenters' recommendations appear promising. For example, a disclosure (*e.g.*, "why did I get this ad?") that is located in close proximity to an advertisement

---

[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;
Nov. 1 Transcript, *supra* note 21, at 200-253 (Session 5: Roundtable Discussions of Data Collection, Use and Protection); Nov. 2 Transcript, *supra* note 23, at 9-94 (Session 6: Disclosures to Consumers).

and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising, could be an effective way to communicate with consumers. Indeed, such a disclosure is likely to be far more effective than a discussion (even a clear one) that is buried within a company's privacy policy. Further, as described above, some businesses have already begun to experiment with designing other creative and effective disclosure mechanisms. Staff encourages these efforts and notes that they may be most effective if combined with consumer education programs that explain not only what information is collected from consumers and how it is used, but also the tradeoffs involved – that is, what consumers obtain in exchange for allowing the collection and use of their personal information.

With respect to the concern about using cookies to allow consumers to exercise their control over whether to allow behavioral advertising, staff encourages interested parties to examine this issue and explore potential standards and other tools to assist consumers. Moreover, as to some commenters' call for guidance on the mechanics of disclosures outside the website context, staff notes that different business models may require different types of disclosures and different methods for providing consumer choice. Staff therefore calls upon industry to develop self-regulatory regimes for these business models that effectively implement the transparency and consumer control principle. Regardless of the particular business model involved, the disclosures should clearly and prominently inform consumers about the practice and provide them with meaningful, accessible choice.

Finally, staff notes that research suggests that it is important to test proposed disclosures to ensure that they serve their intended purpose.[68] Staff therefore encourages stakeholders to

---

[68] *See*, *e.g.*, FTC Bureau of Economics Staff Report, *Improving Consumer Mortgage Disclosures: An Empirical Assessment of Current and Prototype Disclosure Forms* (June 2007),

conduct empirical research to explore the effects of possible disclosures on consumer understanding in this area.

C. Reasonable Security and Limited Data Retention for Consumer Data

Commenters also discussed the second proposed principle, which calls upon companies to provide reasonable security for, and limited retention of, consumer data collected for behavioral advertising purposes.

A number of companies generally supported this principle as drafted. Echoing the arguments raised about the Principles' applicability to non-PII, other companies, as well as industry groups, recommended that the Commission limit the application of this principle to PII. These commenters also called for more flexibility in applying this principle, and stated that data retention should not constitute a separate, stand-alone principle; instead, according to these commenters, data retention should be viewed as one possible component of an effective security program. Several industry commenters suggested that the principle should allow companies to consider various factors in evaluating appropriate data retention periods, and should refrain from imposing a uniform requirement.

Although the consumer groups generally supported this principle as proposed, some argued that the FTC should strengthen certain aspects of the principle. Individual consumers and one privacy group suggested that the principle is too vague and should provide more detailed and precise security standards. Two privacy groups stated that companies should retain data only as long as needed to fulfill the identified use for which the company collected the data. Other

---

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 Project* (Feb. 28, 2006), *available at* http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf.

proposals included a requirement that companies anonymize all retained data, a requirement that data be retained for no longer than six months, and a suggestion that the FTC hold a workshop to explore issues related to the appropriate data retention standard.

For the reasons addressed above, staff believes the Principles should apply to all data collected and used for behavioral advertising that reasonably could be associated with a particular consumer or with a particular computer or device. Staff recognizes, however, that there is a range of sensitivities within this class of data, with the most sensitive data warranting the greatest protection. Accordingly, as proposed, the data security principle stated that, consistent with existing data security laws and the FTC's many data security enforcement actions,[69] the "protections should be based on the sensitivity of the data [and] the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company." Staff believes that this scalable standard addresses the commenters' concerns while also ensuring appropriate protections for consumer data. Staff therefore retains this language in the Principles without change.

Staff agrees with many of the commenters, however, that data retention is one component in the reasonable security calculus, rather than a separate, stand-alone principle, and has clarified the principle to reflect this position. The intent behind the principle remains unchanged, however: companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need. As noted above, over the past year some companies have changed their data retention policies to reduce substantially the length of time they maintain

---

[69] *See, e.g.*, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2002). Information about the FTC's data security program and enforcement actions can be found at http://www.ftc.gov/privacy/.

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 commenters stated that, as proposed, this principle goes beyond FTC case law and existing self-regulatory regimes and statutes. Other commenters expressed concern that this principle will be applied to prospective changes to companies' practices and noted that such changes should, at most, require opt-out consent.

By contrast, consumer and privacy groups, as well as an individual consumer, expressed strong support for this principle as proposed. One consumer organization acknowledged that a business may have legitimate reasons for altering its privacy promises and stated that the principle strikes the proper balance between consumers' interests in reliable promises and industry's need for flexibility. This commenter expressed concern, however, about the use of "pre-checked" boxes and similar mechanisms to obtain opt-in consent, and noted that such

mechanisms might not reflect consumers' actual intent.[70]

It is fundamental FTC law and policy that companies must deliver on promises they make to consumers about how their information is collected, used, and shared.[71] An important corollary is that a company cannot use data in a manner that is materially different from promises the company made when it collected the data without first obtaining the consumer's consent.[72] Otherwise, the promise has no meaning. Staff recognizes, however, that a business may have a legitimate need to change its privacy policy from time to time, especially in the dynamic online marketplace. In addition, minor changes to a company's data practices may be

---

[70] Staff agrees that pre-checked boxes and choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement are insufficient to express a consumer's "affirmative express consent." *See, e.g.*, Deborah Platt Majoras, Chairman, FTC, Remarks at the Anti-Spyware Coalition at 7 (Feb. 9, 2006), *available at* http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf ("[B]urying critical information in the End User License Agreement ("EULA") does not satisfy the requirement for clear and conspicuous disclosure. Buried disclosures do not work."); FTC Publication, *Dot Com Disclosures: Information About Online Advertising* at 5 (May 2000), *available at* http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf ("Making [a] disclosure available . . . so that consumers who are looking for the information *might* find it doesn't meet the clear and conspicuous standard . . . . [D]isclosures must be communicated effectively so that consumers are likely to notice and understand them.") (emphasis in original); *see also* FTC Policy Statement on Deception at Part III, appended to *In the Matter of Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm (fine print disclosures not adequate to cure deception).

[71] *See, e.g.*, *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS (D. Mass. filed July 10, 2000) (alleging that company violated privacy promises); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (alleging that company violated promises about the security provided for customer data); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (same); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (same); *In the Matter of Educ. Research Ctr. of Am.*, FTC Docket No. C-4079 (May 6, 2003) (alleging that company violated privacy promises); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (alleging that company violated privacy and security promises).

[72] *See, e.g.*, *In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004); *see also In the Matter of Orkin Exterminating Co.*, 108 F.T.C. 263 (1986).

immaterial to consumers and may not warrant the costs and burdens of obtaining consumers' consent.

For these reasons, the material change principle is limited to changes that are both *material*[73] and *retroactive*. Depending upon a company's initial privacy promises, a material change could include, for example: (i) using data for different purposes than described at the time of collection, or (ii) sharing data with third parties, contrary to promises made at the time of collection. A retroactive change is a change in a company's policies or practices that a company applies to previously collected data. This would include, for example, the situation where a company makes a material change to its privacy policy and then uses previously collected data in a manner consistent with the new policy, but not the old one. A retroactive change does not include the circumstance where a company changes its privacy policy and then proceeds to collect and use *new* data under the new policy. Staff agrees that the latter type of change – which would constitute a *prospective* change – may not raise the same concerns as a retroactive change, and may therefore call for a more flexible approach.[74]

Staff has revised the material change principle to make clear that it applies to retroactive

---

[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.

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 to receive the advertising. Many of the commenters who discussed this principle raised the issue of how to define the types of information that should be considered sensitive. Some commenters also questioned whether affirmative express consent is the appropriate standard or whether behavioral advertising based on sensitive data should be prohibited altogether.

Various commenters discussed the lack of agreement regarding the definition of "sensitive," and noted that whether specific information is considered sensitive can depend upon the context and the individual consumer's perspective. Other comments – including those filed on behalf of scientific and medical organizations, industry groups, and privacy and consumer advocates – listed specific categories of information that should be considered sensitive. According to these commenters, the categories include information about children and adolescents, medical information, financial information and account numbers, Social Security numbers, sexual orientation information, government-issued identifiers, and precise geographic location.[75]

Despite the lack of agreement on the definition of "sensitive data," there appears to be consensus that such data merits some form of heightened protection. Different commenters,

---

[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.

however, provided differing views on the necessary level of protection. Several individual companies and industry groups objected to an opt-in approach. These commenters stated that opt-in consent for the collection of sensitive data for online behavioral advertising is too burdensome and is unnecessary in light of existing regulatory regimes.[76] Others stated that the uncertainty over how to classify sensitive data makes an opt-in approach difficult to implement and enforce.

Another group of commenters, including business and consumer groups, supported an affirmative express consent standard for certain sensitive data. They reasoned that such a standard strikes the correct balance and would allow those consumers who value advertising based on sensitive information to receive it.

A third group of commenters, including individual consumers, businesses, consumer groups, and a state government agency, supported a ban on behavioral advertising based on sensitive data. These commenters cited the risk of harm from sensitive data falling into the wrong hands. Other commenters recommended banning the use of specific types of sensitive data, such as information about children. Finally, a number of commenters called for additional examination of the issue, including discussion about how to define what constitutes sensitive data.

Given the heightened privacy concerns and the potential for significant consumer harm from the misuse of sensitive data, staff continues to believe that affirmative express consent is

[76] These commenters specifically cited the COPPA Rule (children's information), the Health Insurance Portability and Accountability Act ("HIPAA") (health information), and the GLB Act (financial information).

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 clearest examples, staff encourages industry, consumer and privacy advocates, and other stakeholders to develop more specific standards to address this issue. Staff also encourages stakeholders to consider whether there may be certain categories of data that are so sensitive that they should never be used for behavioral advertising.

F. Secondary Uses

Relatively few commenters responded to the Principles' call for information regarding the use of tracking data for purposes other than behavioral advertising. Most of the industry commenters that did address this question focused on such internal uses as website design and optimization, content customization, research and development, fraud detection, and security. For the reasons discussed above, staff believes that such "first party" or "intra-site" uses are unlikely to raise privacy concerns warranting the protections of the Principles. Other businesses

[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 continues its work on behavioral advertising, it will seek more information on this issue and consider further revisions to the Principles as needed.

IV. REVISED PRINCIPLES

Based upon the staff's analysis of the comments discussing the Principles as initially proposed, and taking into account the key themes enumerated above, staff has revised the Principles. For purposes of clarification, the new language is set forth below in bold and italics. As noted above, these Principles are guidelines for self-regulation and do not affect the obligation of any company (whether or not covered by the Principles) to comply with all

[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.

A. Definition

For purposes of the Principles, online behavioral advertising means the tracking of a consumer's online activities ***over time*** – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests. ***This definition is not intended to include "first party" advertising, where no data is shared with third parties, or contextual advertising, where an ad is based on a single visit to a web page or single search query.***

B. Principles

1. Transparency and Consumer Control

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option. ***Where the data collection occurs outside the traditional website context, companies should develop alternative methods of disclosure and consumer choice that meet the standards described above (i.e., clear, prominent, easy-to-use, etc.)***

2. Reasonable Security, and Limited Data Retention, for Consumer Data

Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the

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.***

3. Affirmative Express Consent for Material Changes to Existing Privacy Promises

As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use ***previously collected*** data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

4. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising

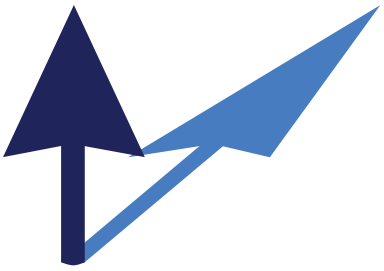
Companies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising.

V. CONCLUSION

The revised Principles set forth in this Report constitute the next step in an ongoing process, and staff intends to continue the dialogue with all stakeholders in the behavioral advertising arena. Staff is encouraged by recent steps by certain industry members, but believes that significant work remains. Staff calls upon industry to redouble its efforts in developing self-regulatory programs, and also to ensure that any such programs include meaningful enforcement mechanisms. Self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences.

Looking forward, the Commission will continue to monitor the marketplace closely so that it can take appropriate action to protect consumers. During the next year, Commission staff will evaluate the development of self-regulatory programs and the extent to which they serve the essential goals set out in the Principles; conduct investigations, where appropriate, of practices in the industry to determine if they violate Section 5 of the FTC Act or other laws; meet with companies, consumer groups, trade associations, and other stakeholders to keep pace with changes; and look for opportunities to use the Commission's research tools to study developments in this area.

The Commission is committed to protecting consumers' privacy and will continue to address the issues raised by online behavioral advertising.



Federal Trade Commission

ftc.gov