Comments of the Center for Democracy & Technology, Consumer Action, and Privacy Activism

In regards to the FTC Staff Statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles"

April 11, 2008

Table of Contents

Executive Summary **3**

Introduction **5**

I. General Comments on FTC Approach **5**
- A. Self-Regulation Versus Other Approaches 5
- B. Costs and Benefits of Offering Consumer Choice 6
- C. FTC Definition of Behavioral Advertising 7
- D. Compliance with the Principles 8

II. CDT Research: Practices of Concern **9**
- A. User Control: Using Flash Cookies to Override User Choice 9
- B. Sensitive Data: User Data Collected on Health Web Sites 12
  - 1. NAI Members Collecting Health Information 13
  - 2. Non-NAI Members Collecting Health Information 14
- C. Behavioral Ad Networks Based on Deep Packet Inspection 15

III. Specific Comments on FTC Principles **18**
- A. Proposed Principle 1: Transparency and consumer control 18
  - 1. Transparency and consumer control should be separate principles 19
  - 2. Including some level of standardization in disclosures would increase their effectiveness. 19
  - 3. Promoting transparency both in browser software and on Web sites may be beneficial. 20
  - 4. Consumer choices should be honored persistently. 21
  - 5. Disclosure of how consumers can exercise control should be explicit 22
  - 6. Potential Principle Revisions 22
- B. Proposed Principle 2: Reasonable security, and limited data retention, for consumer data 23
- C. Proposed Principle 4: Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising 24
- D. Call for additional information: Using tracking data for purposes other than behavioral advertising 25

Conclusion **26**

Executive Summary

The Center for Democracy & Technology (CDT), Consumer Action (CA), and Privacy Activism (PA) welcome the opportunity to comment on the FTC's proposed principles for self-regulation of behavioral advertising. We are pleased that the FTC staff has not foreclosed any regulatory approaches to addressing behavioral advertising concerns despite having issued these principles. We believe that ultimately protecting consumer privacy interests in this space will require a rigorous mix of self-regulation, enforcement of existing law, and a new general privacy law backed up by regulatory enforcement.

In regards to self-regulation, we are encouraged by the release of these principles. The Commission has sent a clear signal that the industry's current self-regulatory framework has been insufficient to protect consumers. Practices on the Internet have moved beyond those anticipated by the current self-regulatory regime. Recent CDT research and information reported in the press confirm that the gaps between current self-regulation and current practices are numerous:

- Current self-regulation does not prohibit companies from overriding a consumer's choice to not be tracked online, and CDT research has revealed that this practice is occurring on the Internet today through the use of "Flash cookies."

- The Network Advertising Initiative (NAI) allows its members to use non-personally identifiable health information for behavioral advertising, but the large and growing number of consumers who search for health information online likely consider this information to be sensitive.

- Companies in the online advertising industry who are not NAI members are not bound by the NAI's notice and choice requirements, allowing them to use health data for behavioral advertising without providing notice and choice, among other things. Consumers whose behavioral information is collected by such companies may have no way of knowing about it and no way of opting out.

- New ad networks appear to be using ISP traffic data for behavioral advertising without proper safeguards or user consent. No regulation or self-regulation exists to address the privacy implications of this new model.

Given this changing landscape, the FTC's proposed principles are a solid first step towards protecting consumer privacy online, but much more work is needed to ensure consumer trust in the important and vibrant online advertising industry that supports Internet content.

CDT, CA, and PA recommend that the FTC strengthen its proposed transparency principle and make consumer control a separate principle. We also suggest that data retention limits be tied to the purpose for which information was collected, and that the FTC host a workshop to explore the appropriate length of time for retaining behavioral data. We agree with the FTC that behavioral advertising based on sensitive data should

require consumer consent, and we suggest that the definition of sensitive data include information about health, finances, sexual behavior, sexual orientation, government-issued identifiers, insurance identifiers, and precise geographic location. Finally, we suggest that more information is needed to understand the secondary uses of behavioral data and how the associated privacy risks should be addressed.

In the FTC's response to the public comments, we urge the Commission to clearly state how it will encourage companies to comply with its principles, whether there will be consequences for failure to comply, whether the Commission will publicly report on industry compliance and if so, the form that reporting will take, and whether a timeline will be imposed for company compliance. Without specific guidance to industry on these matters, we fear that the principles will have little impact and that companies will have little incentive to put the interests of consumers above short-term commercial advancements in behavioral advertising. Such a result would further erode user confidence in the commercial Internet's central business model – advertising-supported content – at the same time that it weakens consumer privacy.

Introduction

The Center for Democracy & Technology (CDT), Consumer Action (CA), and Privacy Activism (PA) are pleased to have the opportunity to submit comments regarding the FTC staff's recent statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles." We believe that the privacy and consumer protection issues raised by behavioral advertising remain an industry-wide concern, requiring ongoing attention from companies, consumers and policymakers, particularly in light of the number of recently announced major mergers and acquisitions of behavioral targeting firms. We thank the FTC for committing to an open dialogue about how best to move forward in this space.

In Section I below we provide general comments on the FTC's approach to behavioral advertising. In Section II we discuss the results of research CDT recently conducted into behavioral advertising practices of concern. Section III provides specific comments regarding the principles that deal with transparency and consumer control, limited data retention, sensitive data, and the use of tracking data for purposes other than behavioral advertising.

I. General Comments on FTC Approach

Our general comments on the FTC's approach discuss self-regulation versus other approaches, the costs and benefits of offering consumer choice, the FTC's definition of behavioral advertising, and compliance with the principles.

A. Self-Regulation Versus Other Approaches

The FTC behavioral advertising Town Hall showcased many new approaches, both self-regulatory and otherwise, for addressing the privacy issues involved with behavioral advertising. CDT, CA, and PA believe that ultimately protecting consumer privacy interests in this space will require a rigorous mix of self-regulation, enforcement of existing law, and a new general privacy law backed up by regulatory enforcement. Thus, we are pleased that the FTC staff "in no way intends to foreclose" ideas and means for protecting consumer privacy that go beyond the statement of proposed principles.[1] We are hopeful that the FTC will indeed continue to consider an array of strategies for addressing this issue. The FTC has a central role to play as efforts in this area move forward on a variety of fronts.

In regards to self-regulation, we are encouraged by the release of these principles. The Commission has sent a clear signal that the industry's current self-regulatory framework is insufficient to protect consumers today. We believe that the Network Advertising

[1] Federal Trade Commission Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 2007), http://www.ftc.gov/os/2007/12/P859900stmt.pdf ("Staff Statement") at 7.

Initiative (NAI)[2] model in particular is inadequate in the specific requirements it sets out for member companies, in the number of companies that have agreed to adhere to the guidelines, and in the level of compliance with the existing guidelines.[3]

B. Costs and Benefits of Offering Consumer Choice

The existence of the NAI is instructive, however, in addressing the FTC's inquiry regarding "the costs and benefits of offering choice for behavioral advertising."[4] We certainly believe that the benefits of choice far outweigh the costs, and that the appropriate position for the leading federal agency charged with protecting consumer privacy online should be in support of choice as well. But perhaps even more telling is the fact that several of the original online behavioral advertising companies committed to providing choice long ago when they crafted the NAI guidelines.[5] More recently, some of the largest companies involved in behavioral advertising have joined the NAI, and in doing so affirmed their support for consumer choice as well. While we have taken issue with the way in which consumer choice has been implemented under the NAI framework, we believe that the companies' voluntary support of choice in principle is strong evidence of its benefits.

Moreover, surveys reveal that many consumers are uncomfortable with behavioral advertising, even when its benefits are explained. In a recently released Harris Interactive/Alan F. Westin study, 59% of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services.[6] A recent TRUSTe survey produced similar results.[7] With such a large proportion of consumers uncomfortable with behavioral advertising, we believe choice is absolutely essential.

---

[2] Network Advertising Initiative, *Network Advertising Initiative Self-Regulatory Principles for Online Preference Marketing By Network Advertisers* (2000), http://www.networkadvertising.org/pdfs/NAI_principles.pdf ("NAI Principles").

[3] *See* Center for Democracy & Technology, *Applying the FTC's Spyware Principles to Behavioral Advertising: Comments of the Center for Democracy & Technology in regards to the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology*" (Oct. 2007), http://www.cdt.org/privacy/20071019CDTcomments.pdf ("CDT Comments"); Center for Democracy & Technology, *Statement of The Center for Democracy & Technology before The Antitrust, Competition Policy and Consumer Rights Subcommittee of the Senate Committee on the Judiciary on "An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks for Competition and Privacy?"* (Sept. 2007), http://www.cdt.org/privacy/20070927committee-statement.pdf.

[4] Staff Statement at 6.

[5] *See Comments of the Network Advertising Initiative: Testimony at the Public Workshop on Online Profiling Sponsored by the Department of Commerce and the Federal Trade Commission* (Nov. 1999), http://www.ftc.gov/bcp/workshops/profiling/comments/nai.htm.

[6] Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings* (Mar. 2008).

[7] "TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting" (Mar. 2008), http://www.marketwire.com/mw/release.do?id=837437&sourceType=1 ("71 percent of online consumers are aware that their browsing information may be collected by a third party for advertising purposes . . .. 57 percent of respondents say they are not comfortable with advertisers using that browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information.").

With clear industry support for choice through its existing self-regulatory programs and consumer concerns over the basic tenets of behavioral advertising, we believe that the remaining question is: how can we give consumers meaningful and effective choices? It was for this reason that we supported the Do Not Track proposal.[8] It is still the only proposal that we have seen that offers consumers a comprehensive, easy-to-use, and durable opt-out control.

In weighing the costs and benefits of behavioral advertising more broadly, several other kinds of analyses would be useful. We have yet to see an independent economic analysis showing that consumers are more likely to click on a behaviorally targeted ad versus an ad targeted based on demographics or the context of the Web page the user is visiting. A sociological study of whether consumers prefer ads targeted based on behavior over other kinds of ads would also be helpful. The FTC should work to promote these kinds of independent research.

C. FTC Definition of Behavioral Advertising

In the background section of the proposed principles, the FTC staff notes its decision to use a broad definition of "behavioral advertising," intended to cover diverse online tracking activities. The definition is as follows:

> [O]nline "behavioral advertising" means the tracking of a consumer's activities online – 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.[9]

Given the diversity of business arrangements and technologies used to deliver targeted advertising, we support the FTC's use of a broad definition. However, for the specific case of contextual targeting – targeting that happens nearly in real time, based only on a consumer's current visit to a single Web page – we think the principles would serve better as a set of best practices as opposed to a set of requirements that all those doing contextual targeting must follow. When a consumer's visit to a single Web page is recorded and used only for the purpose of serving an ad in response to that visit or immediately preceding visits to the same page, the privacy risks associated with the data collection become less pressing. While we would hope that those doing contextual targeting would still abide by the FTC principles, we think making compliance a requirement for those who do pure contextual targeting is unnecessary. Moreover, exempting contextual targeting may help encourage online advertising companies to store less consumer information.

---

[8] *See* Pam Dixon et al, *Consumer Rights and Protections in the Behavioral Advertising Sector* (Oct. 2007), http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.
[9] Staff Statement at 2.

Contextual targeting may arguably be construed to fall outside of the FTC's definition of behavioral advertising if it is not considered to involve "tracking." We believe this distinction should be clarified, however, with the following revisions to the definition (revisions in italics):

> Online "behavioral advertising" means the tracking of a consumer's activities online *over time* – including the searches the consumer has conducted, the web pages visited, and the content viewed – *and/or the storage of records of those activities over time* for the purposes of delivering advertising targeted to the individual consumer's interests.

D. Compliance with the Principles

While the staff statement takes aim at many of the inadequacies of the current self-regulatory principles themselves, it is silent about issues relating to industry compliance with the principles. In the FTC's response to the public comments, we urge the Commission to clearly state how it will encourage companies to comply with its principles, whether there will be consequences for failure to comply, whether the FTC will publicly report on industry compliance and if so, the form that reporting will take, and whether a timeline will be imposed for company compliance.

Without specific guidance to industry on these matters, we fear that the principles will have little impact and that those involved in the online advertising industry will have little incentive to put the interests of consumers above short-term commercial advancements in behavioral advertising. Such a result would further erode user confidence in the commercial Internet's central business model – advertising-supported content – at the same time that it weakens consumer privacy. We have already had one insufficiently enforced self-regulatory framework – we do not need another one.

We also encourage the FTC to articulate benchmarks that will allow both the Commission and outside observers to evaluate the efficacy of the self-regulatory approach. Without such metrics, it will be difficult to judge whether the principles are working to the benefit of consumers. Benchmarks will also provide a rubric for deciding when the guidelines are in need of updating, ensuring that updates happen based on changes in the marketplace rather than solely being based on external regulatory pressure.

II. CDT Research: Practices of Concern

At the Town Hall last fall, the FTC heard about many different kinds of behavioral advertising practices, some of which we believe pose risks to consumer privacy. We wanted to gain a better understanding of how these practices are occurring online to help inform our comments to the Commission. Thus, in early 2008, CDT set out to investigate how certain practices are exhibited on the Internet today.

It is important to note, however, that much of the concern caused by behavioral advertising is based on actions that advertisers and ad networks[10] take on the back-end – how they merge information, who they share it with, and so on. Without access to this information, it is difficult to observe a particular practice and conclude with certainty that the practice poses privacy risks. We cannot know the intentions of an advertiser or an ad network when it collects data. As such, the information we present here is meant to inform the discussion rather than to state specific claims of unfair or deceptive practices.

The practices we highlight below center around two topics addressed in the FTC's proposed principles: user control and sensitive data. We believe that the practices we focus on are not explicitly covered by any current regulation or self-regulatory program, including the NAI. We also include a separate subsection about behavioral ad networks using deep packet inspection; although we did not perform any independent research on this topic, we think it deserves close scrutiny from the FTC.

A. User Control: Using Flash Cookies to Override User Choice

In CDT's comments to the FTC in advance of the Town Hall, CDT described a technique whereby advertisers and advertising networks could use Adobe Flash technology to override a user's decision to delete his or her cookies.[11] CDT decided to focus part of our research on this practice because there is no current regulation or self-regulatory framework that addresses it or other techniques used to circumvent user control.

Flash technology supports what are known as "Flash cookies" (or "local stored objects"), which can be created and accessed by Flash animation objects on a Web site. Flash cookies have similar functionality to regular cookies – they are small files stored on the user's computer to facilitate Web browsing.

The scenario in which Flash cookies may be used to circumvent user control begins with the user visiting a Web site where an ad network sets both a cookie and a Flash cookie containing the same unique identifier. If the user later deletes the regular cookie and returns to the Web site (or any other site where the ad network uses Flash), the ad network can look up the user's Flash cookie and recapture the user's unique identifier.

---

[10] In these comments we use the term "ad network" broadly to describe companies that facilitate Web advertising through ad serving, hosting and ad sales services on the Web.
[11] CDT Comments at 4.

The user can then be associated with this identifier on any site where the ad network requests the user's cookie, whether or not the ad network uses Flash on the site.

We believe this practice unfairly wrests control from users who choose to delete their cookies in order to avoid being tracked. Ad networks use unique IDs to identify the same user or computer across many different Web sites. Users who are aware of this may delete their cookies periodically, believing that the new cookies they receive will contain new unique identifiers, thus hindering the ability of ad networks to track their behavior across sites. Using Flash cookies to re-identify users overrides this control, with little available redress for users. Although users may arguably protect themselves by periodically deleting their Flash cookies as well, the means for doing so are extremely obscure and difficult even for savvy consumers to use.

In February and March 2008, CDT visited a variety of blogs and news sites to determine if ad networks on those sites were using Flash cookies to replace cookie identifiers. On CDT's testing computer, we first identified a group of sites where a single domain was setting both cookies and Flash cookies with the same unique identifier. With a fresh testing computer containing no cookies or Flash cookies on the hard drive, we completed the following process (illustrated in the diagram below):

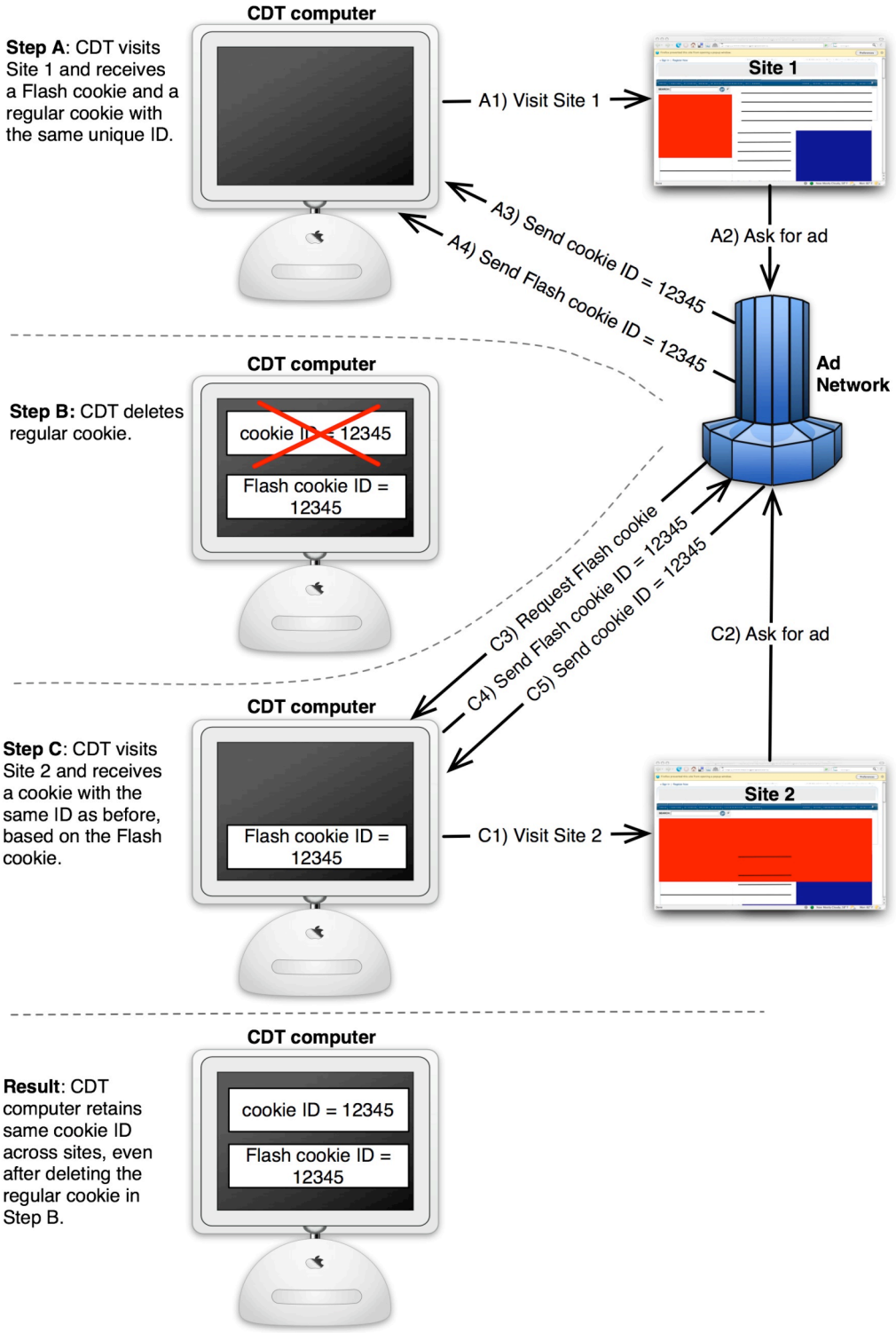
- **Step A:** We would choose one site, say Site 1, to visit. Site 1 would contain content from another domain (perhaps an ad network domain) that would set both a regular cookie and a Flash cookie on our testing computer, both containing the same unique identifier.

- **Step B:** After visiting Site 1, we would delete the regular cookie, but keep the Flash cookie.

- **Step C:** We would then visit another site, Site 2. If the Site 2 visit caused a new cookie to be set from the same domain as the cookie we received when visiting Site 1, we would check to see if the new cookie contained the same identifier as the Flash cookie that was set when visiting Site 1. If this was the case, we could conclude that the Flash cookie was being used to restore the same unique identifier we had obtained when visiting Site 1.

We repeated this test a few times for each domain, with as many different sites as we could find.

Diagram: CDT Flash Cookie Test



Through this process CDT found this practice in use by a company called Mochi Media.[12] Mochi Media provides several different online tools and services, among them an ad network. According to the company Web site, Mochi Media runs MochiAds, "the world's first advertising network for casual games."[13] MochiAds provides a way for developers of online Flash games to insert ads into their games. CDT found that when visiting various Web sites where different MochiAds-supported games could be played, we always received the same cookie ID, identical to the ID stored in a Flash cookie received from a Mochi Media-owned domain.

Of course, we cannot speak to the intentions of Mochi Media in using Flash to re-identify users. We do not know if the company engages in any sort of behavioral advertising, or what data it associates with the persistent unique identifiers it issues to users. Because there is no regulation or self-regulatory framework that addresses this practice, the means for consumers to avoid any tracking conducted by Mochi Media or other companies engaged in this practice are extremely limited.

CDT also found several providers of widget measurement services using this technique. These services allow an online content creator to receive reports about how many Internet users saw and interacted with the creator's widgets, videos, and other Flash-based creations. Although CDT found nothing that indicates that these companies are using Flash cookies to re-identify users for the purpose of behavioral advertising, the existence of these companies demonstrates the reach of this technique across industries.

B. Sensitive Data: User Data Collected on Health Web Sites

CDT chose to research health Web sites since many consumers consider health information to be sensitive but its use for behavioral advertising purposes is not fully addressed by the current self-regulatory regime. Online health information is also a popular topic with Internet users – the Pew Internet & American Life Project reported in 2006 that eighty percent of American Internet users had searched for health information online, and that percentage is likely even higher now.[14]

CDT visited 18 popular health Web sites throughout February and March 2008 to better understand how the information collected on these sites flows between the sites themselves, ad networks, and advertisers.[15] The sample was small, and not meant to be comprehensive. Rather, CDT's goal was merely to get a feel for the online health data collection and sharing landscape. The discussion below is split into two sections dealing

---

[12] We observed this practice on some – but not all – Web sites where we received cookies and Flash cookies from Mochi Media.
[13] *Mochi Media :: Fueling creativity*, http://mochimedia.com/ (last accessed Apr. 1, 2008).
[14] Susannah Fox, *Online Health Search 2006* (Oct. 2006), http://www.pewinternet.org/PPF/r/190/report_display.asp.
[15] The health sites we visited were: about.com/health, cnn.com/HEALTH, drkoop.com, everydayhealth.com, familydoctor.org, health.discovery.com, healthatoz.com, healthline.com, healthstatus.com, healthy.net, mayoclinic.com, medhelp.org, msnbc.msn.com/id/3032076/, realage.com, revolutionhealth.com, steadyhealth.com, yourtotalhealth.ivillage.com, and webmd.com.

with NAI members collecting health information and non-NAI members collecting health information. Although the FTC principles are silent on the distinction between personally identifiable information and non-personally identifiable information,[16] parts of our analysis are predicated on the NAI definitions of these terms, since they are the baseline standards for NAI member companies engaged in behavioral advertising on health sites.[17]

1. NAI Members Collecting Health Information

One of the contours that defines how advertising networks handle health information was set by the NAI, which addresses the use of health information with the following principle:

> Network advertisers shall neither use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, nor social security numbers, for [online preference marketing].[18]

Although this principle prohibits NAI member companies from using personally identifiable information about "sensitive medical data," it allows the use of non-personally identifiable health information for behavioral targeting. Because of concerns over this limited coverage of health information in the NAI, CDT decided to research whether NAI members are collecting non-personally identifiable health information on the Web.

CDT conducted searches on each of the 18 health sites we visited. When a user types a search term into a search box on a Web site, that term is often included as part of the URL of the search results page. For advertising from a third-party ad network to appear on the search results page, this URL is often passed to the ad network as the "referrer" – the page requesting the ad. This helps the ad network deliver the ad directly to the search results page. It also means that the ad network knows the user's search term, since it is included in the referrer URL. If the ad network also requests the user's ad network cookie as part of delivering the ad, the ad network can associate that cookie with the particular search term.

CDT searched for three different terms on each of the sites: "HIV," "diabetes," and "bipolar disorder." With each search, we checked to see if three conditions were met that would demonstrate the transfer of non-personally identifiable health information to NAI members, potentially for behavioral advertising purposes: (1) whether the search results page included content from one or more NAI member companies, (2) whether the referrer

---

[16] We realize that many others will be commenting on the distinction between PII and non-PII as a general matter. We look forward to reading these comments and exploring how new business models may be changing the way the distinction between PII and non-PII can be drawn. We hope the FTC will examine this issue as well.

[17] NAI Principles at 22.

[18] NAI Principles at 3. "Online preference marketing" is defined by the NAI as "a process used by network advertisers whereby data is typically collected over time and across Web pages to determine or predict consumer characteristics or preferences for use in ad delivery on the Web." *See* NAI Principles at 22.

URL contained the search term, and (3) whether the NAI companies requested their cookies identifying CDT's testing computer.

These three conditions were met on 10 out of the 18 sites we visited. This gives us a clear indicator that the collection of non-personally identifiable health information may be a common practice among NAI members.

Again, we do not know how the companies use this information. But there is no regulation or self-regulatory program prohibiting them from using it for behavioral advertising, or from targeting particular users with advertisements based on health searches (e.g., showing lots of ads for mood swing drugs to a user who previously searched for bipolar disorder). Because consumers are searching for health information in ever-growing numbers and the collection of non-personally identifiable health information appears widespread, we believe stronger safeguards are needed in this area, as discussed in Section III.

CDT made one additional noteworthy finding in the course of our searches: one of the health sites we visited contained content from NAI members, but did not provide a link to the NAI opt-out page in its privacy policy.[19] In the absence of a disclosure requirement (the NAI does not require that a link to its opt-out page appear on publisher sites), it appears that this site provides no easy way for users to access their choices about behavioral advertising. Taken together with the fact that collection of non-personally identifiable health information by NAI members may be a common practice, a lack of disclosure about users' choices is alarming.

2. Non-NAI Members Collecting Health Information

Despite the shortcomings of the NAI framework, it does require its members to provide basic notice and choice about certain behavioral advertising activities. But because the principles only apply to NAI members, ad networks that are not NAI members are under no obligation to provide consumers with these protections. In the case of health Web sites, visitors to sites containing behavioral advertising being delivered by a non-NAI members may have no way of finding out how their behavioral health information is being used, and no way to opt out. One indicator of whether this is the case is whether non-NAI members are collecting health information on the Web.

In CDT's survey of 18 health sites, two sites requested content from domains owned by two different ad networks that are not members of the NAI. These sites met the criteria described above – they passed referrer URLs containing sensitive search terms to ad networks that could identify our testing computer's unique cookie IDs. This means that

[19] The privacy policy that did not contain links to the NAI opt-out page was for familydoctor.org (see http://familydoctor.org/online/famdocen/home/about/privacy.html, last accessed Apr. 2, 2008). Even in the full American Academy of Family Physicians privacy policy that the familydoctor.org policy links to, the NAI link does not appear.

on those two sites, health data was undoubtedly collected by a non-NAI member ad network and potentially tied to CDT's unique cookie ID.

Based on information available in the press, it appears that both of the non-NAI networks we observed – AdBrite and Adify – may engage in some behavioral advertising.[20] Thus, it is possible that these two ad networks are using health information for behavioral advertising. Neither of these networks provides an opt-out in its privacy policy, and neither of the two health sites discloses its relationship with the non-NAI network in its own privacy policy or links to the ad network site.[21] Although our sample of 18 sites was small, the fact that we found two sites where non-NAI members were collecting health data is disconcerting given the fact that these companies are under no obligation to disclose their behavioral advertising activities or provide consumers with choice.

C. Behavioral Ad Networks Based on Deep Packet Inspection

In recent months, a new kind of behavioral ad network that accesses and inspects the content of consumer traffic at the Internet Service Provider (ISP) level has been making headlines.[22] In this model, the ad network strikes a deal with an ISP that allows the network to conduct deep packet inspection (DPI) of the individual Web traffic streams of each of the ISP's customers. This means that the ad network receives an individual's Web traffic directly from the ISP and analyzes the content of the traffic in order to create a record of the individual's online behaviors and interests. As customers of the ISP surf the Web and visit sites where the ad network has purchased advertising space, they see ads targeted based on their previous Internet behavior.

---

[20] *See* Phil Leggiere, "Putting Demographics And Behavior In Context," *Behavioral Insider* (Mar. 2007), http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=57450 (AdBrite co-founder Phil Kaplan: "We'll say OK, this visitor is from X zip code so we'll make some educated assumptions about their income demographic and because they're visiting Maxim we'll say there's an 80% probability they're male. Of course if the next 3 sites they go to are Women's Wear Daily, Vogue and another heavily female site, our assumption about gender begins to have to get readjusted. So once you begin doing this for every user for every site they visit, you've soon got a very good working demographic profile based on behavior."); "Everything in its valued place," *Adify Blog* (Feb. 2008), http://blog.adify.com/2008/02/everything_in_its_valued_place.html ("Adify's extensive behavioral targeting capabilities enable our advertisers to define their profiles based on their extensive analytics.").

[21] *See* AdBrite Privacy Policy, http://help.adbrite.com/index.php?action=artikel&cat=2&id=19&artlang=en (last accessed Apr. 2, 2008); Adify Corporation: Privacy Policy, https://app.adify.com/FooterPages/Privacy.aspx (last accessed Apr. 2, 2008); SteadyHealth.com Privacy Act, http://steadyhealth.com/privacy_policy.php (last accessed Apr. 2, 2008) (containing no links to AdBrite or Adify, although both were observed collecting health data and requesting cookies on the site); Healthline Privacy Policy, http://www.healthline.com/privacypolicy.jsp (last accessed Apr. 2, 2008) (containing no link to Adify, although it was observed collecting health data and requesting a cookie on the site).

[22] *See, e.g.,* Peter Whoriskey, "Every Click You Make," *The Washington Post* (Apr. 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule; Saul Hansell, "I.S.P. Tracking: The Mother of All Privacy Battles," *The New York Times: Bits Blog* (Mar. 2008) at http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp=1-b&sq=the+mother+of+all+privacy+battles&st=nyt.

The main difference between these new ad networks – which we will call "DPI-based behavioral ad networks" for lack of a better term – and traditional third-party ad networks is that DPI-based behavioral ad networks may potentially gain access to all or substantially all of an individual's Web traffic as it traverses the ISP's infrastructure, including traffic to all political, religious, and other non-commercial sites. A traditional ad network generally can collect data about a user's behavior only when the user visits the Web sites participating in the network. While today's ad networks may be large, they still do not provide the opportunity to collect information about an individual's online activities as comprehensively as in the DPI model, particularly with respect to activities involving non-commercial content.

The DPI-based behavioral ad networks that have received the most attention recently are Phorm and NebuAd. Based on available information about these companies' practices, we have doubts that operating their systems on an opt-out basis would be consistent with basic consumer protection and privacy principles. There may be other ways of using deep packet inspection for behavioral advertising that would not raise these same concerns, but our doubts about whether consumers are being adequately protected under the DPI model are based on what we know about the companies already operating in this space.

The privacy questions raised by current DPI-based systems are numerous. First, which information gets passed to the ad networks? Although these companies currently inspect predominantly Web traffic, ISPs carry emails, chats, file transfers and many other kinds of data that they could decide to pass on to DPI-based behavioral ad networks in the future. Even if a DPI-based behavioral ad network promises not to record personally identifiable information, many users may still be concerned with a third party receiving this kind of traffic.

Second, what happens when users opt out? The companies listed above offer at least some ISP customers the ability to opt out of the tracking. But in some cases, the traffic of users who have opted out still gets passed to the ad network before being discarded or ignored.[23] The companies also appear to be using cookies – which are susceptible to deletion especially by privacy-conscious users – to store users' opt-out status. Given the comprehensiveness of the Web data these companies can potentially collect, we question the effectiveness of these kinds of opt-out procedures in honoring consumers' choices.

Third, how are consumers notified of the tracking? Disclosure is the privacy aspect of this model that is most difficult to envision in a way that works well for consumers. In some cases, such as Phorm's trials with British Telecom in 2006 and 2007, users were given no notice of the tracking whatsoever.[24] Even when they do aspire towards transparency, DPI-based behavioral ad networks, like traditional third-party ad networks,

---

[23] *See* Chris Williams, "CPW builds wall between customers and Phorm," *The Register* (Mar. 2008), http://www.theregister.co.uk/2008/03/11/phorm_shares_plummet/; Richard Clayton, *The Phorm "Webwise" System* (Apr. 2008), http://www.cl.cam.ac.uk/~rnc1/080404phorm.pdf.

[24] *See* Chris Williams, "BT and Phorm secretly tracked 18,000 customers in 2006," *The Register* (Apr. 2008), http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/; Chris Williams, "BT admits misleading customers over Phorm experiments," *The Register* (Mar. 2008), http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/.

have no direct relationship with consumers. Receiving a privacy notice from a company that is completely unknown to the consumer is likely to be confusing.

ISPs, on the other hand, have strong relationships with their customers, but those involved with DPI-based behavioral ad networks do not appear to be adequately disclosing this involvement. Disclosing this sort of tracking only through a subtle update to the ISP's terms of service is insufficient, and yet that seems to be the path that some of NebuAd's ISP partners are taking.[25] Other kinds of notice that we can envision target only certain groups of an ISP's customers: a notice on the ISP portal home page only works for those who visit that page, and an email only works for those who have provided their email addresses to their ISPs. Notification through banner ads may reach all customers, but the fact that an ISP may be sharing all or a large portion of its customers' Web traffic with a third party is too significant for the disclosure of this fact to occasionally appear in the form of advertisements on Web sites that are wholly unrelated to either the ISP or the DPI-based behavioral ad network. Such disclosures will not garner the attention they deserve from consumers. ISPs may have other disclosure mechanisms, but we have yet to see them used in the DPI-based behavioral ad network context.

Finally, how does the Electronic Communications Privacy Act (ECPA) apply? ECPA, intended to protect the privacy of Internet communications, defines the rights and responsibilities of ISPs with respect to their customers' communications and related data. With certain exceptions, ECPA and its amendments to the federal Wiretap Act prohibit ISPs from intercepting their customers' communications or disclosing the content of those communications to a third party without the customers' permission.[26] This raises two questions: How do the ISPs that have signed up with DPI-based behavioral ad networks justify under ECPA their role in copying or disclosing the content of their customers' communications without prior consent? How do the ad networks justify their obtaining customer communications? The FTC should insist that the ISPs and DPI-based behavioral ad networks already engaged in these practices answer these questions on the record.

In sum, today's DPI-based behavioral ad network practices raise significant privacy risks beyond those posed by the traditional third-party ad network model. The current DPI model defies users' expectations by granting access to potentially the entire range of their Web communications to a third party with whom the users have no relationship. Although the DPI model we have described here is the only one we know of that currently makes this possible, it is worth noting that any behavioral advertising model that captures all or substantially all of an individual's Web traffic or packet streams may very well raise the same issues.

---

[25] *See* Mike Masnick, "Where's The Line Between Personalized Advertising And Creeping People Out?," *TechDirt* (Mar. 2008), http://www.techdirt.com/articles/20080311/121305499.shtml; Peter Whoriskey, "Every Click You Make," *The Washington Post* (Apr. 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule.

[26] *See* 18 U.S.C. 2511 and 18 U.S.C. 2702(b). Other portions of ECPA may also apply.

We believe that any action the FTC takes should address the DPI model. Without answers to the questions raised above – about what information is shared, how opt outs are treated, how users are notified, and how ECPA applies – we have serious concerns about how consumer privacy will be protected as this model evolves. If implementations of the DPI model continue on their current path – or if ECPA demands it – these DPI-based behavioral ad networks should be held to an opt-in only standard, requiring an individual's affirmative express consent prior to collecting an his or her full packet stream for behavioral advertising.

III. Specific Comments on FTC Principles

This section provides specific comments regarding the proposed principles that deal with transparency and consumer control, limited data retention, sensitive data, and the use of tracking data for purposes other than behavioral advertising. Where appropriate, we have proposed specific revisions to the FTC principles that reflect our suggestions (revisions are in italics).

A. Proposed Principle 1: Transparency and consumer control

Concerns about transparency and consumer control were raised repeatedly at the Town Hall. We are pleased that the FTC specifically proposed a principle that would alleviate many of these concerns if it were implemented:

> 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.[27]

CDT, CA, and PA have five recommendations about how this principle could be improved: (1) transparency and consumer control should be separate principles, (2) including some level of standardization in disclosures would increase their effectiveness, (3) promoting transparency both in browser software and on Web sites may be beneficial, (4) consumer choices should be honored persistently, and (5) disclosure of how consumers can exercise control should be explicit. At the conclusion of this section, we have suggested some revised language for this principle that addresses our comments below.

[27] Staff Statement at 3.

1. Transparency and consumer control should be separate principles.

The FTC's first proposed principle recognizes two fundamental concepts underlying consumer privacy: transparency and consumer control. We suggest that given the importance of both concepts, and the differences between them, transparency and consumer control each warrant their own principle, rather than a single principle that groups them together.

This separation makes sense for several reasons. First, generally speaking, consumer control is only meaningful when notice is present. Without knowing how they may exercise their choices, it is hard for consumers to take control of their privacy. Consumer control is thus reliant on transparency, much in the way that the third proposed principle, "Affirmative express consent for material changes to existing privacy promises," is dependent upon transparency. Transparency forms the cornerstone on which consumer control – and several of the other principles – are built, which makes having a principle dedicated solely to transparency much clearer conceptually.

Second, the nature of behavioral advertising causes consumer control to be sufficiently important to warrant its own principle. Much of the data collection involved in behavioral advertising happens automatically as consumers navigate the Web – in most cases consumers are not presented with a choice up front about whether they want to participate. Because of this, designers of behavioral advertising systems have little incentive to provide robust consumer controls. Dedicating a principle solely to consumer control will highlight the importance of providing simple mechanisms that allow consumers to exercise choice.

Finally, the FTC itself has acknowledged the conceptual separation between transparency and consumer control in its explanation of the Fair Information Practice (FIP) principles.[28] While the FIPs deal strictly with the use of personal information, the Notice/Awareness and Choice/Consent principles correlate in many respects to the proposed transparency and consumer control principle from the behavioral advertising guidelines. Separating transparency from consumer control in the behavioral advertising principles is a logical progression from the FTC's previous formulation of these concepts.

2. Including some level of standardization in disclosures would increase their effectiveness.

As the FTC noted in the staff statement, the Town Hall provided much evidence of the fact that consumers do not understand privacy-related disclosures. We believe that the FTC's proposal to have "clear, concise, consumer-friendly, and prominent" statements about behavioral advertising is a helpful step towards raising consumer awareness of behavioral advertising and its potential privacy implications.[29]

---

[28] Federal Trade Commission, *Fair Information Practice Principles* (last modified June 2007), http://www.ftc.gov/reports/privacy3/fairinfo.shtm.
[29] Staff Statement at 3.

To make the FTC's proposed disclosures even more effective, however, we believe that an element of standardization would be helpful. Across the entire Web, there is largely only one standard privacy-related disclosure that consumers come across again and again: the words "Privacy Policy" displayed along the edge of a Web page. Unfortunately, as described by researchers at the Samuelson Clinic at UC-Berkeley and the Annenberg Public Policy Center at UPenn, many consumers believe that having the words "Privacy Policy" on a Web site indicates that the site will not share the consumer information it collects with other companies.[30] This is obviously a grave misconception, but it also points to the power that a standard disclosure can have. If Web sites had a uniform way to say to site visitors, "we are collecting data about you for use in providing targeted advertising" – and if consumers understood this disclosure correctly, as opposed to the "Privacy Policy" case – then over time, consumer awareness of behavioral advertising could be improved. Some level of standardization may also help with other content in a site's disclosure, including information about consumer choices and how to exercise them, as well as other elements of a disclosure such as its format or location on the page.

This is not to say that all disclosures about behavioral advertising should be standardized. But by introducing an element of uniformity, and endeavoring to ensure that any standard disclosures have the appropriate connotation in the minds of consumers, those conducting behavioral advertising may find more success in raising consumer awareness than they have to date. CDT, CA, and PA strongly urge the FTC to begin an industry-wide conversation about how to make this happen.

3. Promoting transparency both in browser software and on Web sites may be beneficial.

We applaud the FTC for proposing that transparency be exercised by "every website where data is collected for behavioral advertising."[31] By including disclosures on all sites across the Web that engage in behavioral advertising, consumers may finally begin to understand the full scope of behavioral advertising and how many different sites it entails. We believe that Web sites may not be the only suitable vehicles for disclosing behavioral advertising information, and that the FTC should consider promoting transparency through Web browser software as well.

What all Web sites that use behavioral advertising have in common is the fact that they are displayed to consumers through Web browsers. The browser may thus be a logical place where behavioral advertising disclosures could be displayed in a "clear, concise, consumer-friendly, and prominent" way.[32] Just as with the "lock" icon in most browsers that signifies an encrypted Web connection and links to an informational display when

---

[30] Joseph Turow, Deirdre K. Mulligan, and Chris Jay Hoofnagle, *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace* (Oct. 2007), http://www.law.berkeley.edu/clinics/samuelson/annenberg_samuelson_advertising-11.pdf.
[31] Staff Statement at 3.
[32] Staff Statement at 3.

clicked, a behavioral advertising disclosure could be accessed through a simple icon or other interface in the browser. This would obviously require Web sites to somehow communicate the necessary information to browser software so that the browser may display it. Using the browser as the disclosure display mechanism may also aid in the development of uniform disclosures, as described above.

We do not necessarily see disclosure through the browser as a substitute for disclosure on Web sites themselves – for some sites one option may be more appropriate than the other. However, we believe the FTC can supplement the current proposed principle by also encouraging disclosures in browser software.

4. Consumer choices should be honored persistently.

When a consumer chooses to opt out of behavioral advertising, that choice should be honored until the consumer decides to opt back in. Offering consumers choices does little good if the results of those choices do not last.[33] If the method for maintaining the opt-out is less than robust – such as in the case of opt-out cookies – opt-out preferences that get lost or deleted should be refreshed. And consumers should have a simple way to learn what their opt-out status is. All of these ideas can be expressed concisely in the FTC principles by requiring that consumer choices be honored persistently and available for consumers to view and change at any time.

The issue of circumventing consumers' decisions can also be addressed with a requirement to honor consumer choices persistently. In addition to the use of Flash cookies to override consumer choice (as discussed in Section I), CDT's comments to the FTC in advance of the Town Hall highlighted a number of other technical means that companies can use to override consumers' choices to opt out of behavioral advertising.[34] We believe that any company engaged in behavioral advertising and seeking to act in good faith should be willing to commit to refraining from overriding consumers' choices. Given the fact that few consumers understand or are even aware of the technical tools available to companies to both track consumer behavior online and override consumers' choices, we believe the expression of this commitment is important enough to be included in the FTC principles.

---

[33] The FTC has supported the persistence of choice in the context of the Do Not Call registry. Although the registry was set to expire after five years, the FTC agreed to keep consumers' phone numbers on the list, in part because of the registry's ability to "enhance the privacy of the American public in a tangible way." *See Prepared Statement of the Federal Trade Commission: "Enhancing FTC Consumer Protection in Financial Dealings, with Telemarketers, and on the Internet"* (Oct. 2007), http://www.ftc.gov/os/testimony/071023ReDoNotCallRuleEnforcementHouseP034412.pdf.

[34] CDT Comments at 3-6.

5. Disclosure of how consumers can exercise control should be explicit.

The proposed principle requires both a statement that "consumers can choose whether or not to have their information collected" for behavioral advertising and a "clear, easy-to-use, and accessible method for exercising this option."[35] While this language may imply that an explanation of how consumers can exercise their choice would be disclosed, there is no explicit requirement that instructions or a link to access the method used to exercise choice be provided. CDT, CA, and PA recommend that this requirement be made explicit to ensure that consumers have a clear, simple explanation of how they may choose not to participate in behavioral advertising.

6. Potential Principle Revisions

The revised principle language below reflects the comments made in this section. The comment about standardization of disclosures is not incorporated below because we view that idea as more of an industry-wide initiative involving dialogue between the FTC and interested parties, as opposed to a specific requirement that could be laid out in the principles.

Our suggested transparency principle:

> Every Web site 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 statement should contain instructions about how consumers may exercise this choice and/or a link that allows consumers to do so. This statement may alternatively be displayed through the consumer's Web browser software.*

Our suggested consumer control principle:

> *Every Web site where data is collected for the purpose of behavioral advertising should provide consumers with a clear, easy-to-use, and accessible method that gives consumers control over whether their data can be collected for this purpose. A consumer's choices expressed using this method should be (1) available for the consumer to view and change, and (2) persistently honored until the consumer decides to alter those choices.*

[35] Staff Statement at 3.

B. Proposed Principle 2: Reasonable security, and limited data retention, for consumer data

CDT, CA, and PA believe that the proposed principle on reasonable security is sufficient to address the concerns raised at the Town Hall. Our comments focus on the proposed limited data retention principle:

> Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.[36]

In the background section of the staff statement, the FTC expresses concern about consumer behavioral advertising data "being used for unanticipated purposes."[37] We believe that the FTC could better guard against unanticipated uses if the limited data retention principle tied data retention to the purposes for which the data was collected in the first place. This formulation would help ensure that the data is kept only as long as necessary to complete the task for which it was collected.

We also believe that as a best practice the limited data retention principle should accommodate a consumer's affirmative choice to have data retained. Although the costs of doing this may be prohibitive in some situations, companies should strive to honor consumer requests to have their data retained.

To incorporate both of these ideas into the limited data retention principle, we suggest the following revision to the first sentence of the principle:

> Companies should retain data *for the minimum time* necessary to fulfill *the purposes for which it was collected. When possible, companies should accommodate a consumer's affirmative choice to have his or her data retained.*

Even with such an updated principle, questions remain about what the appropriate data retention time is for behavioral advertising data. We suggest that the FTC hold a workshop on the topic to explore the length of time for which different kinds of information remain useful and the business reasons for which companies retain behavioral advertising data. Although there has been some public discussion of these questions specifically with respect to search data, we believe a broader inquiry that encompasses other kinds of data is necessary

[36] Staff Statement at 4.
[37] Staff Statement at 2.

C. Proposed Principle 4: Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising

The proposed principle on sensitive data is as follows:

> Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.[38]

We believe the FTC has struck the right balance by requiring affirmative express consent for behavioral advertising using sensitive data. This practice undoubtedly makes some consumers uncomfortable, but others may wish to receive advertisements targeted to sensitive data categories. Requiring affirmative express consent allows for both of these cases while providing the necessary safeguards by default.

The FTC is also seeking further input on the principle:

> FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice.[39]

We suggest the following definition of sensitive data for the behavioral advertising context:

Sensitive data consists of:

- information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information;
- financial information;
- information about an individual's sexual behavior or sexual orientation;
- Social Security Numbers or any other government-issued identifiers;
- insurance plan numbers; and
- information indicating the precise geographic location of an individual when he or she accesses the Internet.

We believe these are the classes of data that most consumers might consider sensitive. Most of these data types are given some sort of special treatment in at least one U.S. statute or self-regulatory program.[40] While precise geographic location information has received less attention than some of the others listed, we believe location information carries particular significance in the behavioral advertising realm because more and more

[38] Staff Statement at 6.
[39] Staff Statement at 6.
[40] Congress and the states have also afforded special protections to records of what consumers watch on cable television, the books they borrow from the library, and the videos they rent from the video store. In developing its approach to sensitive data, the FTC should consider the interplay between these laws and its guidelines for behavioral advertising.

consumers are accessing the Internet from mobile devices capable of reporting their specific physical locations. Location information should be treated as sensitive not only because consumers may be particularly uneasy about ads targeted to their immediate vicinity, but also because the collection of location information by a third party has potentially serious privacy consequences from a physical tracking perspective.

Beyond the definition of sensitive data, there are two additional requirements that are needed to complete this principle. It will not suffice for companies to obtain consumer consent to use "sensitive data" if consumers do not understand what "sensitive data" consists of. Thus, companies should be required to obtain consent to use each of the sensitive data categories. In addition, companies should obtain consent directly from consumers themselves – consent provided to one company should not be transferable to other companies.

With the inclusion of these changes, the revised principle would be as follows:

> A company should only collect sensitive data for behavioral advertising if it obtains affirmative express consent *directly* from the consumer to receive such advertising. *Sensitive data consists of: information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information; financial information; information about an individual's sexual behavior or sexual orientation; Social Security Numbers or any other government-issued identifiers; insurance plan numbers; and information indicating the precise geographic location of an individual when he or she accesses the Internet. Companies should obtain affirmative express consent for each category of sensitive data they intend to use for behavioral advertising.*

D. Call for additional information: Using tracking data for purposes other than behavioral advertising

The FTC's call for additional information on secondary use is as follows:

> FTC staff seeks additional information about the potential uses of tracking data beyond behavioral advertising and, in particular: (1) which secondary uses raise concerns, (2) whether companies are in fact using data for these secondary purposes, (3) whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data, and (4) whether secondary uses, if they occur, merit some form of heightened protection.[41]

CDT, CA, and PA are pleased that the FTC is seeking additional information on this topic, because evidence of behavioral advertising data being used for secondary purposes is largely anecdotal. Although there have been some reports of companies using

[41] Staff Statement at 6.

behavioral data for price discrimination,[42] it is unclear how widespread this practice is. Other uses – sharing or selling behavioral data, or using it to make credit or insurance decisions, for example – are largely undocumented, but would raise serious concerns if they were shown to be occurring. Based on the Town Hall meeting and our own conversations with online advertising players, we believe that it is unlikely that the FTC will garner enough information through the comment process about what secondary uses are occurring and which parties are involved. Therefore, we believe the Commission should seek additional information specifically on this topic, whether through a workshop or an additional written proceeding.

An additional level of complexity around the secondary use question is arising as the line blurs between what were traditionally known in the behavioral advertising context as "first parties" and "third parties." For example, many ad networks are moving to a model where they serve ads directly from publisher domains. Whereas previously an Internet user visiting Example-Publisher.com (the "first party") might receive ads (and cookies) from the Example-Ad-Network.com domain (the "third party"), now the user may receive ad network content from Example-Ad-Network.Example-Publisher.com, or another domain hosted by Example-Publisher.com. In this case, if behavioral information was collected to allow for better ad targeting on Example-Publisher.com, and then Example-Ad-Network decides to use the data for some separate purpose, should that separate use be considered secondary? More information is needed to understand how data flows in relationships like these, and which uses can appropriately be considered primary and secondary.

In general, we have the fewest concerns about behavioral advertising conducted by a first-party publisher with whom a consumer has an established relationship. But arrangements like the one described above blur the distinction between first parties and third parties, making it difficult not only to determine which data uses are secondary, but generally which privacy safeguards should be provided by each of the different parties involved. Investigating how to draw a distinction between first parties and third parties may be a useful endeavor for the FTC to pursue, and we would be happy to work with the Commission on that effort.

Conclusion

CDT, CA, and PA are pleased to be a part of the FTC's open dialogue about how best to address the privacy issues raised by behavioral advertising. The issuance of the FTC's proposed principles affirms our belief that the current self-regulatory framework has failed to protect consumer privacy. In the absence of a general privacy law, the FTC must address not only the practices of concern that companies are already engaged in, but also the potential threats to privacy that will continue to emerge as technologies and business models evolve. The FTC's proposed principles are a promising start, but much more work is needed – and much more information about how behavioral advertising is

[42] *See* Louise Story, "Online Pitches Made Just For You," *The New York Times* (Mar. 2008), http://www.nytimes.com/2008/03/06/business/media/06adco.html.

actually taking place – before consumers will be sufficiently protected online. Ultimately, as the Commission concluded in its July 2000 report to Congress on this issue, "backstop legislation addressing online profiling is still required to fully ensure that consumers' privacy is protected online."[43]

For more information, contact Alissa Cooper at acooper@cdt.org or 202-637-9800 x110.

[43] Federal Trade Commission, *Online Profiling: A Report to Congress* (July 2000), http://www.ftc.gov/os/2000/07/onlineprofiling.htm.