ONLINE BEHAVIORAL ADVERTISING: INDUSTRY’S CURRENT SELF-REGULATORY FRAMEWORK IS NECESSARY, BUT STILL INSUFFICIENT ON ITS OWN TO PROTECT CONSUMERS

December 2009

This report analyzes the current behavioral advertising frameworks of the Federal Trade Commission, Network Advertising Initiative, Interactive Advertising Bureau and Privacy Group Coalition (none of which have been comprehensively implemented as of this paper’s release) and provides CDT’s recommendations for protecting consumers in this space.

Table of Contents

EXECUTIVE SUMMARY .................................................................................................................. 3
I. INTRODUCTION .......................................................................................................................... 6
II. SCOPE OF REGULATORY FRAMEWORKS ............................................................................... 7
   A. DEFINING ONLINE BEHAVIORAL ADVERTISING ................................................................. 8
      1. Addressing Behavioral Trackers Who Collect and Use All or Substantially All Internet Traffic Content ............................................................................................................. 9
   B. WHAT DATA ARE COVERED BY THE FRAMEWORKS? ...................................................... 10
      1. How to Approach Sensitive Data? ....................................................................................... 11
   C. CONCLUSION: TIME TO TAKE THE NEXT STEPS .......................................................... 13
III. TRANSPARENCY .................................................................................................................... 13
   A. NOTICE ................................................................................................................................ 13
      1. Where is Notification? ........................................................................................................... 13
      2. Content of Notification and Disclosures ............................................................................. 16
      3. Notification by Behavioral Trackers Who Collect and Use All or Substantially All Internet Traffic Content ............................................................................................................. 17
   B. CHANGES TO PRIVACY POLICIES .................................................................................... 18
   C. PRETEXTING .......................................................................................................................... 19
IV. INDIVIDUAL PARTICIPATION .................................................................................................. 20
   A. “SEEKING INDIVIDUAL CONSENT” .................................................................................. 20
      1. Persistence of the Opt-out and Better Browser Controls ...................................................... 21
      2. What Kind of Control? ......................................................................................................... 22
      3. Sensitive Data ....................................................................................................................... 23
      4. Merged Data ........................................................................................................................ 24
      5. Behavioral Trackers Who Collect and Use All or Substantially All Internet Traffic Content .......................................................................................................................... 24
   B. “MECHANISMS FOR APPROPRIATE ACCESS, CORRECTION, AND REDRESS” ............. 25
V. PURPOSE SPECIFICATION ......................................................................................................... 28
VI. DATA MINIMIZATION ................................................................................................................ 29
A. REDUCING DATA COLLECTION .............................................................................. 29
B. DATA RETENTION LIMITS .................................................................................. 30

VII. USE LIMITATION ............................................................................................. 31
A. SECONDARY USES OF DATA ............................................................................ 31
B. TRANSFERRING BEHAVIORAL DATA ................................................................ 32

VIII. DATA QUALITY AND INTEGRITY .................................................................. 33

IX. SECURITY ............................................................................................................. 33

X. ACCOUNTABILITY AND AUDITING ................................................................. 34
A. COMPLIANCE WITH THE PRINCIPLES ......................................................... 35
B. REDRESS ............................................................................................................. 36

XI. CONCLUSION ..................................................................................................... 37
Executive Summary

The Center for Democracy & Technology (CDT) recognizes that advertising is an important engine of Internet growth. Consumers clearly benefit from a rich diversity of content, services and applications that are provided without charge and are supported by advertising revenue. However, as sophisticated new behavioral advertising models are deployed, it is vital that consumer privacy be protected. Massive increases in data processing and storage capabilities have allowed advertisers to track, collect and aggregate information about consumers' Web browsing activities and compile individual profiles used to match advertisements to consumers' interests. All of this is happening in the context of an online environment where more data is collected – and retained for longer periods – than ever before. It is time to assess where consumer privacy stands in this ecosystem and what needs to be done.

This report concludes that, although progress has been made in expanding self-regulatory efforts, self-regulation alone will continue to be insufficient to adequately protect consumers in regards to behavioral advertising. Not only do recently revised self-regulatory principles still fall short even as written, but the online advertising industry has historically failed to fully implement its self-regulatory principles. Moreover, no self-regulatory system is likely to cover or be enforced against all entities, especially when new participants enter and leave the scene. In its February 2009 report, the Federal Trade Commission staff did not foreclose regulatory approaches to addressing behavioral advertising concerns. CDT strongly believes now is the time for Congress and the FTC to play a larger role to ensure that consumer interests are fully protected.

We believe that fully protecting consumer privacy interests here will require Congress to pass general consumer privacy legislation that encompasses both the online and offline space and to give the FTC broader rulemaking authority over consumer privacy in general and behavioral advertising practices more specifically. Once the appropriate legal framework has been constructed, companies can work within this space to adopt self-regulatory guidelines appropriate to their business models. Self-regulation can only effectively work when we have baseline legislation and regulatory authority to provide a meaningful backbone.

In addition, we conclude that self-regulatory guidelines, Federal legislation and FTC rulemaking should reflect the full set of Fair Information Practice principles (FIPs). Properly understood, FIPs constitute a comprehensive privacy framework. Unfortunately, most privacy schemes to date have focused on only a subset of FIPs; some have been radically confined only to notice and consent. In this report, CDT calls for application of the full set of FIPs and presents the following concrete recommendations:

- **Transparency**
  - Consumers have the right to clear, prominent and meaningful notification about how their personal information is being collected and used.
  - Notice should occur distinct from privacy policies and terms of service. Notice should be located on every Web page where such data collection or use occurs and should link to more comprehensive disclosures.
To optimize the effectiveness of any notification scheme, an element of standardization in notifications and disclosures should be implemented.

Notice that links to a trade association Web site is insufficient. Notices should link to information that describes the specific companies that are tracking the consumer, including any companies tracking the consumer through an advertisement, the companies that have contributed data about the consumer to behaviorally target the advertisement, and other data collection objects on the Web site the consumer is visiting.

The content of disclosures should be clear and comprehensive.

The FTC and all self-regulatory programs should prohibit the practice of pretexting (gathering information from consumers through games or sweepstakes) without an unavoidable and clear notice and clear consent based on an understanding of potential privacy costs.

- **Individual Participation**
  - Every Web site where data is collected for the purpose of behavioral advertising should either provide consumers with a clear, easy-to-use opt-in or a centralized, comprehensive and easy-to-use means to opt-out of data collection and use.
  - A consumer’s choice should be (1) available for the consumer to view and change, and (2) persistently honored until the consumer decides to alter his or her choices.
  - The definition of sensitive data should be broader than it is in current self-regulatory frameworks; collection of sensitive data about an individual should require express affirmative opt-in consent.
  - We should move the discussion beyond the terms personally identifiable information and non-personally identifiable information. This binary distinction does not reflect the complexity of this issue. Instead, we should focus on a continuum of data – identifiable, pseudonymous and aggregate data.
  - At a minimum, three specific standards should be applied to behavioral trackers who collect all or substantially all Internet traffic content in order to target individuals: (1) unavoidable notice and affirmative, express opt-in consent, (2) ongoing notice, and (3) revocable consent. The burden is on those who wish to move forward with this behavioral advertising model to demonstrate that these standards can work in this context.
  - When a consumer has limited options, Internet service should not be contingent on “opting-in” to data collection for behavioral advertising purposes.
  - Consumers should be able to access, and delete or correct, data that is being collected about them and the profiles being constructed in connection with behavioral advertising.

- **Purpose Specification**
  - All disclosures about data collection and use practices should include clear, prominent and meaningful notice about how collected data will be or is being used. Collection for any and all purposes does not per se meet this test.
• **Data Minimization**
  o The collection and aggregation of consumer data should be minimized.
  o Data retention should be tied to the purpose for which the data was collected.

• **Use Limitation**
  o The use of behavioral advertising data for secondary purposes raises serious concerns and the FTC should follow up on its earlier plan to seek additional information specifically on this subject.
  o All transfers of behavioral data, whether to affiliate or non-affiliate entities, should be transparent and specified in advance to consumers.
  o CDT supports the FTC’s “Affirmative Express Consent for Material Changes to Existing Privacy Promises” principle, but we must ensure that the term “material” does not become meaningless.

• **Data Quality and Integrity**
  o Consumer profile access is the best mechanism for ensuring data quality and integrity.

• **Security**
  o Proper implementation of the FTC’s security guidelines will sufficiently protect consumer data.

• **Accountability and Auditing**
  o Any self-regulatory approach should be girded by legislation and FTC enforcement.
  o We encourage the FTC to articulate benchmarks that will allow both the Commission and outside observers to evaluate the efficacy of self-regulation.
  o Compliance reviews must be public and conducted by independent third parties.
  o There must be meaningful consequences for failure to comply with these FIP principles.

We hope this report will not just move the discussion forward, but serve as a call for swift and more meaningful action in this space. Consumers deserve no less.
I. Introduction

In February 2009, the Federal Trade Commission (FTC) issued a staff report outlining self-regulatory guidelines for the online advertising industry. The guidelines, which offer an “ongoing examination of online behavioral advertising,” are organized along principles of “Transparency and Consumer Control,” “Reasonable Security, and Limited Data Retention for Consumer Data,” “Affirmative Express Consent for Material Changes to Existing Privacy Promises,” and “Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising.”  

Upon the release of the staff report, FTC commissioner (now FTC Chair) Jon Leibowitz warned industry that the guidelines were not to be ignored. “Put simply,” he said, “this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers’ privacy in a dynamic online marketplace.”

To some industry groups, the message came in loud and clear. In July 2009, the Interactive Advertising Bureau (IAB) released a “Self-Regulatory Program for Online Behavioral Advertising” intended to correspond with the principles laid out by the FTC and to be implemented by year’s end. The Network Advertising Initiative (NAI), which published its own “Self-Regulatory Code of Conduct” in December 2008, two months before the release of the FTC’s staff report, has published a slideshow comparing its guidelines with those promulgated by the FTC.

In September 2009, ten advocacy organizations released their own set of guiding principles to address behavioral advertising and called for federal legislation in the face of “failed self-regulatory efforts.” These organizations, collectively the “Privacy Group

---

Coalition,” recommend legislation built around a detailed framework of Fair Information Practice principles (FIPs), such as those put forth by the Department of Homeland Security in December of 2008. The principles outlined by these ten organizations essentially comport with the DHS FIPs.⁸

In response to these developments, the Center for Democracy & Technology (CDT) surveyed the current behavioral advertising regulatory frameworks, and now we offer our own set of recommendations to move the discussion forward. To this end, this report analyzes the current behavioral advertising frameworks of the FTC, NAI, IAB and Privacy Group Coalition (none of which have been comprehensively implemented as of this paper’s release) and provides CDT’s suggestions for protecting consumers in this space. An overarching theme in this analysis is our belief that any discussion of online and offline privacy must be grounded by a comprehensive set of FIPs.⁹ The FIPs have been embodied in varying degrees in the Privacy Act, Fair Credit Reporting Act, and the other “sectoral” federal privacy laws that govern commercial uses of information online and offline. CDT strongly believes that the concept of FIPs has remained relevant for the digital age despite the dramatic advancements in information technology that have occurred since these principles were first developed. We believe that the most recent government formulation of the FIPs offers a relevant and robust set of modernized principles that should serve as the foundation for any discussion of self-regulation or legislation. While we begin with a discussion of the scope of regulatory frameworks in this space, our analysis is centered on the FIP principles as laid out by DHS in 2008:

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing

II. Scope of Regulatory Frameworks

CDT Recommendation: Protecting consumer privacy interests in the context of behavioral advertising requires a rigorous mix of self-regulation, enforcement of existing law, and enactment of a new consumer privacy statute that establishes baseline protections and gives the FTC rulemaking authority. We need self-regulatory frameworks based on a comprehensive set of FIPs, but self-regulation can only effectively work

---


⁹ For a more detailed discussion of what CDT is looking for in comprehensive privacy legislation, see Center for Democracy & Technology, Refocusing the FTC’s Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable (Nov. 2009), available at http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf.
when we have consumer privacy legislation and effective enforcement to provide a meaningful backbone.\textsuperscript{10}

The February 2009 FTC staff report outlines revised self-regulatory guidelines, or principles, for the online advertising industry. When it released the report, the FTC recognized that “significant work in this area remains” and that the principles only represented a step in an ongoing process to evaluate self-regulatory programs.\textsuperscript{11} The FTC did not foreclose any regulatory approaches to addressing behavioral advertising concerns and sent a clear signal that the industry’s existing self-regulatory framework had been insufficient to protect consumers.

\textit{A. Defining Online Behavioral Advertising}

\textbf{CDT Recommendation:} The definition of online behavioral advertising, hereafter referred to as “behavioral advertising,” must not be used as a tool to shield questionable practices from privacy regulation. The definition should be broad enough to cover diverse online tracking activities. CDT believes that contextual advertising, however, is distinct from behavioral advertising, as it poses fewer privacy risks and better aligns with consumer expectations about how data is being collected and used and therefore may need a different set of protections.

The FTC’s proposed self-regulatory principles apply broadly to companies engaged in online behavioral advertising.\textsuperscript{12} Like the FTC principles, the NAI, IAB and Privacy Group Coalition principles do not generally include contextual advertising – targeting based only on a user’s current visit to a single Web page – within the definition of behavioral advertising. CDT agrees that there should be a distinction made between contextual and behavioral advertising. Contextual advertising typically falls within the reasonable expectations of the user – the user has chosen to go to the site and would likely anticipate seeing an ad or personalized content responsive to the nature of his or her actions on the site. Assuming that the data is only used by the site, not stored for other uses and not shared with third parties, the privacy risks associated with this form of data collection become less pressing.

However, CDT is concerned that both the NAI and IAB principles significantly limit the scope of practices that should be considered behavioral advertising and thus shield a large swath of practices from coverage by their own self-regulatory frameworks. The NAI, for example, distinguishes between “Online Behavioral Advertising,” “Multi-Site Advertising” and “Ad Delivery & Reporting.” According to the NAI’s definition, Online Behavioral Advertising refers only to the practice of using collected data to “categorize

\textsuperscript{10} See id.


\textsuperscript{12} Staff Report at 20. The Staff Report defines online behavioral advertising as “tracking consumers’ online activities over time . . . in order to deliver advertising that is 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.” Staff Report at 20.
likely consumer interest segments.”

So-called Multi-Site Advertising covers a much broader set of data collection and use practices that also pose privacy risks. However, while the NAI has extended nearly all of its principles (i.e., notice, transfer and service restrictions, access, reliable sources, security, and data retention) to cover Online Behavioral Advertising and Multi-Site Advertising, the NAI has neither established a choice requirement for Multi-Site Advertising nor specifically applied its use limitations principle to Multi-Site Advertising. CDT had hoped this gap would be closed as the NAI proceeded with its implementation guidelines, but thus far it has not been.

Similarly, CDT is concerned that the IAB guidelines do not apply to third-party entities that are collecting data from sites with which they are affiliated. For example, DoubleClick, which is owned by IAB member company Google, could track individuals on Web sites owned by Google – such as Gmail, Google Books, YouTube, and Blogspot – without providing any notifications or mechanisms for control and regardless of the information’s sensitive nature. The NAI’s definitions of Online Behavioral Advertising and Multi-Site Advertising appear to allow a similar practice since they apply only to data collected “across multiple web domains owned or operated by different entities.”

In contrast to the NAI and IAB, the Privacy Group Coalition does not appear to limit the definition of online behavioral advertising in any significant way.

1. **Addressing Behavioral Trackers Who Collect and Use All or Substantially All Internet Traffic Content**

**CDT Recommendation:** *Regulatory efforts must expressly address behavioral trackers who collect all or substantially all Internet traffic content in order to target individuals. This behavioral advertising model requires heightened protection. At a minimum, three specific standards should be applied to behavioral trackers who collect all or substantially all Internet traffic content in order to target individuals: (1) unavoidable notice and affirmative, express opt-in consent, (2) ongoing notice, and (3) revocable consent. The burden is on those who wish to move forward with this behavioral advertising model to demonstrate that these standards can work in this context.*

In the past year, new models of behavioral advertising have been proposed that involve the participation of ISPs, toolbars and software. One particularly intrusive model uses deep packet inspection (DPI) techniques to analyze consumer communications as they move over the network of an ISP. Ad networks that partner with ISPs, toolbars or software could potentially collect and record every aspect of a consumer’s Web

---

13 NAI Principles at 4.

14 See IAB Principles at 10-11.

15 NAI Principles at 4.

16 Legislative Primer at 11 (defining “behavioral targeting” as “the practice of collecting and compiling data from and about an individual’s activities, interests, preferences, behaviors, or communications for interactive advertising and marketing targeted to the individual, including but not limited to the use of a profile that may be stored or linked to a browser cookie, IP address, or any other persistent user identifiers or tracking methods. Behavioral targeting does not include contextual advertising.”).
browsing, including every Web page visited, the content of those pages, how long each page is viewed, and what links are clicked. Emails, chats, file transfers and many other kinds of data could all be collected and recorded.\textsuperscript{17} Access and inspection of the content of consumer traffic at this level raise very serious questions and, in some cases, may violate wiretapping and related laws.\textsuperscript{18}

Despite the specific concerns raised by this type of behavioral advertising and the growing consensus that affirmative consent would be needed for such practices, the FTC principles do not set out any special guidance for behavioral advertising that is based on data collected by the monitoring of all or substantially all Internet traffic data. The NAI has promised to pursue an implementation guideline that outlines requirements for companies engaged in this practice, but thus far, it has not done so. The Privacy Group Coalition also does not directly address this troubling issue in its framework.\textsuperscript{19}

On the other hand, the IAB makes its principles specifically applicable to data collected by ISPs, toolbars, browsers, and other desktop applications or software that “[collect and use] data from all or substantially all URLs traversed by a web browser across Web sites for Online Behavioral Advertising.”\textsuperscript{20} This is a step in the right direction.

\textbf{B. What Data Are Covered by the Frameworks?}

\textbf{CDT Recommendation}: Regulation must protect any type of data that can be used to identify, contact, or locate an individual. For behavioral advertising uses, the distinction between PII and non-PII is too simplistic and should no longer be central to the privacy framework in this space. Instead, we should focus on a continuum of data – identifiable, pseudonymous and aggregate data.

For years, privacy debates have swirled endlessly around discussions of what constitutes “personally identifiable information” (“PII”) versus non-personally identifiable information (“non-PII”). The underlying issue, however, is much more complex than these terms suggest. In its staff report, the FTC properly began to move away from this distinction. Instead, the FTC included within the scope of its Principles “any data collected for online behavioral advertising that reasonably could be associated with a


\textsuperscript{19} The Coalition’s definition of “behavioral targeting” does, however, include “the use of a profile that may be stored or linked to a . . . IP address.” Legislative Primer at 11. It is CDT’s understanding that the Privacy Group Coalition did not specifically address this concern in the primer because it was operating on the assumption that it is already illegal for ISPs to engage in behavioral tracking and targeting based on customers’ browsing, emails, etc.

\textsuperscript{20} IAB Principles at 11.
particular consumer or computer or other device," regardless of whether the data is "personally identifiable" in the traditional sense. CDT believes this phrasing represents a significant change in the discourse. Researchers have consistently shown that a data record about an individual, even after the removal of traditional identifiers, is rarely anonymous. Thus, we believe the term “anonymous” is often misleading to consumers. Collected data should be evaluated on a spectrum that ranges from identifiable data to pseudonymous data (in which some identifying information has been removed) to aggregated data. Principles that guide data collection, protection, and use practices should appropriately reflect the pseudonymity of the data. We plan to examine this complex issue in more detail in a follow-up paper.

The Privacy Group Coalition agrees with the FTC here and generally follows this practice in its Legislative Primer. That is, any information that enables an individual to be distinguished as a particular computer user is included within the scope of its recommended consumer privacy legislative framework. In contrast, both the NAI and IAB self-regulatory approaches rely on the simplistic distinction between PII and non-PII. The definitions of PII outlined by the NAI and IAB both fail to account for information that can be used to identify, contact, or locate an individual.

1. How to Approach Sensitive Data?

CDT Recommendation: The extra level of protection afforded sensitive data should be granted, at a minimum, to:

• Information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information of an individual;
• Financial information about an individual;
• Information about an individual’s sexual behavior or sexual orientation;
• Social Security Numbers or any other government-issued identifiers;
• Insurance plan numbers;

21 Staff Report at 25.


24 Legislative Primer at 4.

25 See NAI Principles at 5; IAB Principles at 11.

26 See NAI Principles at 5; IAB Principles at 11.
• **Information indicating the precise geographic location of an individual when he or she accesses the Internet.**

The FTC, NAI, IAB, and Privacy Group Coalition vary significantly in their treatment of sensitive data. In its report, the FTC does not directly define what constitutes sensitive data and instead encourages interested parties to develop their own detailed standards. Nevertheless, the Commission highlights what it considers to be clear examples of sensitive data – financial data, data about children, health information, precise geographic location information and Social Security numbers. The Privacy Group Coalition believes sensitive data should include “data about health, finances, ethnicity, race, sexual orientation, personal relationships and political activity” and provides detailed definitions of financial information and health information, which we find commendable. The Coalition calls on the FTC, as opposed to Congress, to ultimately outline and enforce a definition.

The NAI offers a potentially broad definition of sensitive information in its principles, one that comports with many of CDT’s recommendations. For example, the NAI definition of sensitive data includes precise geographic location information and a broader definition of health information. However, the NAI notes that the definition of sensitive information will be further developed in an implementation guideline; thus far, such a guideline has not been adopted. If the NAI chooses to significantly narrow the sensitive information definition through this process – or if NAI member companies continue to use health, location, and other sensitive data categories for behavioral advertising while they wait for the implementation guideline to be completed – then the gains exhibited in the current NAI principles will be hollow. Little progress seems to have been made on this important issue. CDT urges the NAI to maintain a broad definition of sensitive information.

The IAB sensitive data definition seems narrow. We urge the IAB to expand its definition of sensitive data to a far larger set of data types.

---

27 In CDT’s 2009 Threshold Analysis for Online Advertising Practices, we subdivide location data into five categories: civic location data, geodetic location data, mobile location data, fixed location data, and nomadic location data. We believe that all mobile location data, fixed location data, and nomadic location data is sensitive in nature. Geodetic location data and civic location data can be sensitive depending on the precision of the data. Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), available at http://www.cdt.org/privacy/20090128threshold.pdf.

28 Staff Report at 43-44.

29 Legislative Primer at 4. Financial information includes “[a]ny information, regardless of source, about an individual’s income, wealth, investments, or bank or other financial accounts.” Health information includes “[a]ny information, regardless of source, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; and the past, present, or future payment for the provision of health care to an individual.” Id. at 12.

30 NAI Principles at 6.

31 IAB Principles at 17 (“financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual”).
C. Conclusion: Time to Take the Next Steps

The FTC’s February 2009 principles were a promising start, but much more needs to be done to adequately afford consumers the full privacy protections outlined in a comprehensive FIPs model.

We remain skeptical, however, that even the most comprehensive self-regulatory framework would be adequate to fully police behavioral advertising practices. As we have set out before, self-regulation is necessary but not sufficient to provide consumers with adequate safeguards. It must operate in concert with enforceable law.\textsuperscript{32}

III. Transparency

Entities should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of information.\textsuperscript{33}

A. Notice

1. Where is Notification?

\textbf{CDT Recommendation:} Consumers have the right to clear, prominent, and meaningful notification that their data is being collected or used for behavioral advertising. The best way to achieve this is to provide a concise notice on every Web page where such data collection or use occurs, and on every ad delivered on the basis of behavioral data, with a link to detailed information about what data is being collected (or used), by whom, how it will be stored, transferred, and used, how users can opt-out of such data collection, and how they can contact data collecting entities to review and correct information that has been collected about them.

For too long, “notice” of data collection and use policies has been provided only in a privacy policy or a terms of service, where information most relevant to the consumer is buried in detailed legalese. Research shows that consumers almost never read these privacy policies or terms of service. Moreover, research shows that most users, when they see the hyperlinked words “Privacy Policy” on a Web site, assume that they mean that their information is not being collected or shared, even if the policy says just the opposite.\textsuperscript{34} It is time to move beyond this approach and use, on the page where the collection occurs, more effective language, such as “Data Collection Practices.”

\textsuperscript{32} See The Privacy Implications of Online Advertising: Hearing Before the Senate Comm. on Commerce, Science & Transportation, 110th Cong., 1st Sess. (July 9, 2008) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology) (addressing the shortcomings of self-regulation).

\textsuperscript{33} DHS FIPs. We have italicized the DHS FIP principle at the beginning of each section discussing a specific principle.

The FTC, NAI, IAB, and Privacy Group Coalition each recommend that all Web sites on which data is collected for the purposes of behavioral advertising include notice of collection practices. Each guideline, however, suggests different mechanisms by which such notice should be provided.

The FTC’s framework provides the least specific guidelines. The staff report requires that “[e]very Web site where data is collected for behavioral advertising should provide notice,” and that such notice should be “clear, concise, consumer-friendly and prominent.” The FTC encourages innovative approaches to notification beyond privacy policies and also explains that “different business models may require different types of disclosures.”

The NAI Code is similarly vague with respect to notice, stating that each member engaged in behavioral advertising must ensure that notice is “available on the website where data are collected for OBA and/or Multi-Site Advertising Purposes.”

The NAI has stated in testimony:

The NAI 2008 Self-Regulatory Code requires its members to secure notice and choice for consumers on the Web sites on which their behaviorally-related advertisements appear. While as a practical matter such notice and choice is usually provided within a Web site’s privacy policy (or a layered summary of the policy), the Code allows NAI members the flexibility to pursue any disclosure approach so long as companies ensure that clear and conspicuous notices are available to consumers on the websites where online behavioral advertising occurs.

Further, “the NAI and its member companies believe that technologies should be developed and built to allow for enhanced notice by any entity engaged in online behavioral advertising” and are now taking positive steps working to this end. Although CDT is encouraged by these efforts, we continue to have concerns about how companies will implement the framework.

By contrast, the IAB guidelines suggest a series of mechanisms that, if implemented correctly, will help ensure that all consumers are appropriately notified of the ways in which information about them and their online activities is being collected. The IAB requires that “clear, meaningful, and prominent” notification, with a link to a disclosure, must be “[o]n or around” the place on the Web page where data is collected or elsewhere on the Web page, in space donated by the publisher.

---

35 Staff Report at 35-36 (“Staff therefore encourages companies to design innovative ways – outside of the privacy policy – to provide behavioral advertising disclosures and choice options to consumers.”).

36 NAI Principles at 7.


38 Id.

a “clear, meaningful, and prominent” link to more information, instead of equating notice and the longer disclosure, the IAB makes such on-page (as opposed to just on-site) notification possible. Moreover, this requirement ensures that even if data is collected through means other than an advertisement, for example by a Web beacon (a 1x1 tracking pixel) on a publisher’s Web site, customers are notified of the activity. The IAB’s emphasis on “Web page” instead of “Web site” is significant: notification on a “Web site” can be a line in a privacy policy. Notification on a “Web page” means notice on each and every page where data is collected: such notice will be far more accessible to users. Although we are encouraged by the IAB’s framework for notification, we have yet to see any implementation of it.

Like the IAB, the Privacy Group Coalition recognizes the need for notification outside the privacy policy, and they suggest a mechanism similar to the IAB’s. The Coalition recommends that “[w]ebsites and other online services collecting user data must clearly and prominently provide on their ads – via linked webpages as well as within privacy policies – a consumer-friendly explanation of their data collection practices.” Yet the Coalition seems to limit such notice requirements to data collectors who place ads on a given Web site; it does not address the need for notice of collection undertaken by Web beacons placed by companies not actually advertising on the Web site.

While the current landscape of self-regulation might mean that different Web sites are governed by different standards (IAB, NAI, etc.), 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 notices and disclosures could be displayed in a “clear, concise, consumer-friendly, and prominent” way. Just as the “lock” icon in most browsers signifies an encrypted Web connection and links to an informational display when clicked, a behavioral advertising disclosure could be accessed through a simple icon or other interface in the browser. This would require agreement among Web sites that engage in behavioral data collection to communicate the necessary information to browser software and it would require browser developers to create an icon and a place in the browser frame where it would appear. In this situation, the browser would control whether or not to display an icon based on the meta data submitted. We do not, however, necessarily see disclosure through the browser as a substitute for disclosure on Web sites themselves.

Using the browser as one disclosure display mechanism may also aid in the development of uniform disclosures and uniform controls for protection within the browser.

Consumers would be greatly aided by more standardization in the way notices and disclosures are presented, in order to promote both transparency and accountability. To

---


41 Legislative Primer at 8.
begin with, scripting tags that identify who is serving each advertisement or each beacon should be standardized; some companies are moving in this direction and those efforts should be encouraged. At present, determining the source or sources of any advertisement or data-collecting object requires both technological savvy and a time-commitment that are unreasonable to expect from the average user. Some level of standardization may also be appropriate for various aspects of the behavioral advertising disclosures, including the presentation of consumer choices and how to exercise them, as well as other elements of a disclosure such as its format or location on the page. Research into how to effectively communicate online advertising practices to consumers, such as that being undertaken by the Future of Privacy Forum, will help illuminate best practices for consumer notification.42

2. Content of Notification and Disclosures

CDT Recommendation: Although we favor standardized elements in disclosures, as this may help consumers understand the data collection process and how they can exercise choice, all disclosures must clearly state which company or companies are collecting and using personal data, including data provided by advertisers, third-party data suppliers, and any ad networks collecting or using relevant data along the ad delivery chain. A key tenet of transparency requires informing consumers exactly who is tracking them and what type of information each respective tracker is collecting. It is imperative that consumers are told which companies are employing behavioral targeting, the specific practices of each company involved in tracking, and the process by which consumers can go to access the profiles that are being created about them.

As discussed above, the term “notification” can refer to a few paragraphs within a privacy policy or to a link on or around an advertisement. But whether “notice” of data collection consists of a few words or a few paragraphs, the FTC, NAI, IAB, and Privacy Group Coalition each specify that such notice should either include or link to a more comprehensive disclosure of how data is being collected and used. The published standards for disclosure content, however, vary considerably.

The FTC Principles only require advertisers to state that personal data is being collected and to state that consumers can opt-out of data collection.43 The Privacy Group Coalition’s disclosure requirement is similar; the Coalition’s Legislative Primer suggests that an entity engaged in behavioral targeting “must have a publicly available privacy policy that describes its practices and policies with respect to the collection, maintenance, use, and disclosure of information about an individual used for behavioral targeting.”44 The NAI and IAB both require that disclosures outline the type of data to be collected, how the data will be used or transferred, and a link to a mechanism for


43 Staff Report at 46.

44 Legislative Primer at 9.
exercising control over data collection. The IAB disclosure also must list which PII is being collected,\textsuperscript{45} while the NAI requires that members list additional information on their Web sites, including the length of the data retention period and the types of PII and non-PII that will be merged.\textsuperscript{46} CDT is encouraged by the NAI and IAB’s disclosure requirements, but the key questions are whether they will be comprehensively implemented by the end of the year deadline, and whether or not they will be interpreted by members as requiring the comprehensive disclosure of individual companies responsible for tracking. Multiple companies are typically involved in the targeting of a particular ad, including the advertiser in the case of retargeting, data aggregators providing data to the advertiser directly or through demand-side platforms or ad exchanges, and then downstream ad networks that use behavioral data to optimize audience as the ad is relayed to the consumer. Any solution that elects one of these constituents to be identified in notice to the exclusion of others should be viewed as inadequate.\textsuperscript{47}

3. Notification by Behavioral Trackers Who Collect and Use All or Substantially All Internet Traffic Content

\textbf{CDT Recommendation:} Entities not traditionally engaged in online targeting, such as ISPs, toolbars and software that collect behavioral data, should provide consumers with unavoidable notice about their data collection practices. Absent comprehensive transparency, consumers simply do not expect that any entity is able to collect all or substantially all Internet traffic content to be looking into the content of their Internet activities.

\textit{At a minimum, three specific standards should be applied to behavioral trackers who collect all or substantially all Internet traffic content in order to target individuals: (1) unavoidable notice and affirmative, express opt-in consent, (2) ongoing notice, and (3) revocable consent. However, the burden is on those who wish to move forward with such a model to demonstrate that these standards can work in this context. Moreover, when consumers have limited options for Internet access, ISPs should not require that consumers “consent” to such data collection as a prerequisite for using their services.}

ISPs are a critical part of the chain of trust that undergirds the Internet; giving an unknown third party broad access to all or most consumer activity will likely undermine that trust. Similarly, consumers do not expect that the toolbars and software they download are tracking their every click online. The use of all or substantially all Internet traffic content for behavioral advertising defies consumer expectations about what happens when they surf the Web and communicate online. Finding out that there is a

\textsuperscript{45} IAB Principles at 12 (“notice should include clear descriptions of the following: (a) The types of data collected online, including any PII for Online Behavioral Advertising purposes.”).

\textsuperscript{46} NAI Principles at 7 (“Such notice shall include clear descriptions of the following, as applicable . . . The types of PII and non-PII that will be merged . . . the approximate length of time that data used for OBA, multi-site advertising and/or ad delivery & reporting will be retained by the member company.”).

\textsuperscript{47} There has been some encouraging work by companies in the compliance area to address some of these concerns. For example, see Better Advertising, http://www.betteradvertising.com/index.html (last visited Dec. 3, 2009).
middleman lurking between consumers and Web sites they visit would come as an unwelcome surprise to most Internet users.

Only the FTC and the IAB refer to the responsibilities of entities that track all or substantially all consumer behavior online. The FTC’s staff report emphasizes that “[w]here 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.).” The IAB explicitly requires that these entities post “clear, meaningful, and prominent” notice on their Web sites that “describe the types of data collected and their uses, as well as an easy to use mechanism for” (opt-in) control over the collection, use, or transfer of data. CDT is cautiously optimistic about the IAB’s efforts to address these next-generation behavioral advertising techniques, but we reserve judgment until the IAB implements these standards. We are eager to see whether and how “unavoidable notice” and other CDT recommendations are incorporated into the notice and consent process.

B. Changes to Privacy Policies

CDT Recommendation: The concept of transparency is built upon a recognized right of consumers to make informed decisions about how personal information can be collected and used. However, if changes are made to policies that govern how previously collected information can be used, then consumers’ right to informed consent is violated. To resolve this problem, entities must notify consumers of material changes to data use practices; only upon receiving consumers’ opt-in consent should entities use data collected under the previous set of policies. For this system to function, however, the scope of what is considered a “material change” needs to be clear. The FTC should clarify the meaning of the term “material change” and strictly enforce this standard.

The responsibility to provide notice extends beyond the time of data collection. The FTC guidelines state that “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.” The IAB mirrors the FTC on this point, while the NAI guidelines only require that “[i]f a member changes its own privacy policy with regard to PII and merger with non-PII for OBA, prior notice shall be posted on its website.” This is insufficient for three reasons. First, it only covers the merger of PII with so-called non-PII, a distinction that CDT believes, and the FTC agrees, is too simplistic. Second, the mere posting of information on a company’s Web site is not adequate “notice” in this context, especially given the minimal probability that consumers will be routinely monitoring each member company’s Web site for

---

48 Staff Report at 46.

49 Staff Report at 47 (emphasis in original).

50 IAB Principles at 3.

51 NAI Principles at 9.

52 Staff Report at 21-25; see also Barbaro & Zeller, Jr., supra note 22 (AOL incident highlights the difficulties in making data truly anonymous).
changes. And third, this guideline only covers practices the NAI defines as “Online Behavioral Advertising” and does not cover the Multi-Site Advertising that represents a significant segment of the broader behavioral advertising space.

The Privacy Group Coalition recommends that any changes in a behavioral targeter’s privacy policy must be preceded by 30 days of notice on the advertiser’s Web site as well as “specific notice to any person who has requested notice of privacy policy changes.” This solution provides privacy conscious consumers with the opportunity for notification without creating a hassle for consumers that are not as privacy aware. However, the Privacy Group Coalition goes farther than any of the other frameworks, recommending that the policy on changes not be limited only to “material” changes; instead, the Coalition states that “[a]ny change to a privacy policy that has the effect of allowing additional uses or disclosures of information about an individual may apply only to information collected after the effective date of the change.” CDT does not currently believe such a blanket requirement is necessary – alerting individuals to any change of purpose, no matter how minor, for behavioral data could likely be counterproductive to enhancing privacy protection. The concept of “material change” as introduced in the Gateway Learning Corp. case can provide sufficient protection to consumers so long as companies do not try to give “material change” too narrow a reading. The FTC should provide more guidance on when a material change has occurred.

C. Pretexting

CDT recommendation: CDT believes that pretexting represents a deceptive practice. Although we were encouraged by the FTC’s criticism of pretexting in its settlement with Sears Holding Corp., we would like to see pretexting prohibited by the FTC and the trade associations.

Pretexting refers to the practice of asking consumers for personal information or encouraging spyware downloads under the pretext of a benefit such as sweepstakes or coupons without unavoidable and clear notice and consent based on an understanding of the potential privacy costs of participating.

Only the Privacy Group Coalition addresses the use of pretexting as a method to obtain user information. The Privacy Group Coalition recommended legislation that forbids

53 Legislative Primer at 9.

54 Legislative Primer at 9.


57 Legislative Primer at 7-8 (“No forms of pretexting can be used to obtain user information. For example, a contest that seeks the collection of consumer information in exchange for the chance to win a prize is a pretext.”).
pretexting. CDT believes that this is an area that the FTC should investigate. The FTC should bring cases under the FTC Act.

IV. Individual Participation

Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.

A. “Seeking Individual Consent”

CDT Recommendation: 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 choice 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 that choice.

CDT has long identified individual participation, and its subparts such as “consumer control,” as an essential element of any regulatory framework. Without a mechanism for opting out of data collection, privacy-conscious consumers are left with one unpalatable option: logging off.\(^\text{58}\)

CDT agrees with sentiments expressed by Representative Rick Boucher\(^\text{59}\) that all sharing for behavioral targeting purposes should be opt-in, unless a company that is not collecting all or substantially all data about consumers’ online activities is a member of a self-regulatory regime with an easy-to-find, easy-to-use, centralized and persistent opt-out.

The FTC has also emphasized the importance of consumer choice mechanisms, requiring that consumers have “clear, easy-to-use, and accessible” ways to exercise choice with regard to general data collection. While the FTC does not clearly spell out whether such a mechanism should be opt-in or opt-out, by leaving the details of such a mechanism to individual companies, the Commission has basically given a tacit approval to opt-out approaches.

The NAI and IAB outline somewhat more specific guidelines. The IAB offers a basic mechanism by which consumers can opt out of behavioral targeting, and the NAI provides such a mechanism for data collected for “Online Behavioral Advertising.” This mechanism does not apply to data collected for so-called “Multi-Site Advertising,” which is indeed a type of online behavioral advertising, even if the NAI chooses not to identify it as such. (As discussed earlier, the NAI defines OBA as advertising that involves the

---

\(^{58}\) See GREG CONTI, GOOGLE SECURITY: HOW MUCH DOES GOOGLE KNOW ABOUT YOU? (2009).

categorization of “likely consumer interest segments for use in advertising online.” Multi-Site Advertising involves all other instances in which behavioral tracking data is collected and used for advertising purposes.)

The Privacy Group Coalition suggests a completely different framework. According to its recommendations, Web sites should only initially collect and use data from consumers for a 24-hour period, with the exception of information categorized as sensitive, which should not be collected at all. Any subsequent use or collection of non-sensitive consumer data must have the affirmative consent of the individual user, including specific consent for any sale or other sharing of the data. Additionally, the Coalition is the only group to recognize that consent might be best coupled with an expiration date; it recommends that “[a]ny consent for the collection of information for behavioral targeting purposes must be recent (e.g., within three months) and revocable. Once consent has expired or been revoked, information collected with consent must be deleted promptly.”

1. Persistence of the Opt-out and Better Browser Controls

CDT Recommendation: Consumer opt-outs need to be implemented using technologies that will protect the persistence of the opt-out. Companies engaged in behavioral advertising should promise not to override consumers’ choices. Opt-out cookies are not persistent and should be discouraged. Also, consumers should have a simple way to determine what their opt-out status is.

Furthermore, opt outs must protect users from all forms of data collection; the use of “Flash cookies” to collect behavioral information after the user has deleted traditional cookies is of particular concern. A mechanism that blocks traditional cookies but does not interfere with Flash cookies is not an effective “opt-out” mechanism. The use of tracking techniques that intentionally circumvent user control should be prohibited as inconsistent with FIPs. Developers of Web browsers should be encouraged to innovate and create more advanced and comprehensive consumer controls for privacy.

Even though the existence of an opt-out mechanism is a step in the right direction, such controls often rely on technologies that are insufficiently robust. For example, the NAI’s Web site uses the discredited mechanism of opt-out cookies: cookies are placed on a user’s Web browser to indicate his or her opt-out status, but if the user, in an attempt to protect his or her privacy, deletes all cookies, then he or she loses the opt-out status as well. The NAI has released a beta version of a Firefox browser add-on that protects these opt-out cookies from inadvertent deletion. However, such a tool only protects the opt-out cookies placed on the Firefox browser; it does not resolve the concerns raised by relying solely on opt-out cookies to protect against tracking. It is, however, a step in the

---

60 NAI Principles at 7-8; IAB Principles at 12-14. The IAB states: “The opportunity for Web site users to exercise choices about whether Web viewing data can be collected and used for online behavioral advertising will never be more than a few clicks away from such standardized wording and link/icon.” Id. at 5.

61 Legislative Primer at 7.

right direction. The IAB, whose self-regulatory principles were released in July 2009, has yet to implement an organization-wide opt-out mechanism.63

Self-regulatory guidelines should include a clear commitment to honor consumer choices persistently. At present, consumers do not have the knowledge or tools to ensure that their choices are preserved.

CDT urges the adoption of persistent opt-outs through browser controls and other technologies. We also urge the industry to discourage tracking techniques, such as Local Stored Objects (Flash cookies), that circumvent user control.64 It is important to note that Google and Microsoft are both NAI and IAB members and both browser manufacturers. These companies could work with others to build the tools for persistent opt outs into the browser.

2. What Kind of Control?

CDT Recommendation: Consumers should have the ability to control the collection of all personal information, not merely data that is described as PII.

Framing the debate over individual participation as one between opt-in and opt-out is overly simplistic. A centralized and easy-to-use opt-out mechanism can be far more effective than an “opt-in” buried in a terms of service. Moreover, a mechanism is not effective whether framed as opt-out or opt-in if it only covers so-called “personally identifiable information.” The distinction between personally identifiable and non-personally identifiable information does not reflect the complexity of this issue;65 as the FTC’s guidance states, “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 itself, determine the protections provided for consumer data . . . both PII and non-PII raise privacy issues.”66

63 This is also an issue worldwide. The consumer Web site the IAB has set up in the United Kingdom suggests that some members will use opt-out cookies that are not persistent. The site informs consumers that some providers use opt-out cookies while “some providers’ opt out is persistent and some provide a plug-in.” IAB, Your Online Choices: A Guide to Online Behavioral Advertising, Opt Out Help, http://www.youronlinechoices.co.uk/opt-out/opt-out-help (last visited Oct. 16, 2009).

64 For example, Laurie Sullivan recently reported in Media Post that when new IAB member Tattoo Media “began to develop its core behavioral frameworks and algorithms, it believed Flash cookies would remain the best way to slow the ability of consumers to delete cookies from their computers.” Tattoo Media’s Web site advertises that the company tracks users for a longer period of time than do most behavioral targeters. See Laurie Sullivan, Moving Flash Cookies into Direct-Response BT, MediaPost Blogs (Sept. 16, 2009), http://www.mediapost.com/publications/?art_aid=113594&fa=Articles.showArticle (last visited Oct. 30, 2009).


66 Staff Report at 21-25.
In broader terms, different standards for what is achieved by an opt-out can create significant problems in a self-regulatory ecosystem. For example, consumers will likely be confused by the meaning of opt-out if members of one trade association offer a comprehensive opt-out that protects against all types of longitudinal data collection while members of another group offer a less comprehensive opt-out.

Any discussion of opt-out technologies begs an important question: what, exactly, will consumers be able to opt-out of? The NAI requires that “[t]he level of choice . . . shall depend on the manner in which data is intended to be used. Choice is commensurate with the increased privacy implications of data to be used.” Furthermore, the NAI provides no mechanism for opting-out of the collection of data for so-called Multi-Site Advertising. While CDT agrees with the NAI that greater data sensitivity requires more granular, stringent controls, we are concerned that the NAI’s “commensurate control” policy will, in practice, give consumers some choice over the collection and use of personally identifiable information but no choice concerning the collection and use of ostensibly non-personally identifiable information.

3. Sensitive Data

CDT Recommendation: We believe the FTC has struck the right balance by requiring affirmative express consent for behavioral advertising using sensitive data, and we are encouraged that the IAB regulations track the FTC principles here. We caution against efforts to reduce collection of data from adolescents, for such restrictions may result in Web sites instituting practices that deprive at-risk adolescent Internet users of the ability to access important services and information.

The use of sensitive data for behavioral advertising 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.

The FTC, NAI, IAB, and Privacy Group Coalition each recognize that sensitive data, which can range from Social Security numbers to health information, requires special protection and each details additional mechanisms for consumer control over such data. The FTC and IAB only permit the collection of sensitive data following consumers’ opt-in consent; the NAI requires opt-in consent for data collection for “Online Behavioral Advertising” purposes, but not for the collection of data that will support “Multi-Site Advertising.”67 The Privacy Group Coalition goes a step further in suggesting that under no condition should sensitive information be collected for the purposes of behavioral advertising.68

67 Staff Report at 47; IAB Principles at 17; NAI Principles at 8.
68 Legislative Primer at 4.
The NAI, IAB, and Privacy Group Coalition each prohibit, to varying degrees, behavioral advertising targeted at children. The NAI and IAB, in line with the requirements set forth in the Children’s Online Privacy Protection Act (COPPA), restrict certain data collection from children under the age of 13.

The Privacy Group Coalition goes further and suggests prohibiting the collection and use of behavioral data from children and adolescents under the age of 18. As we have seen with service providers’ efforts to comply with COPPA, very few online services can afford to undertake any “parental consent” process. Instead, many sites have simply taken steps to exclude children from their sites altogether. CDT strongly disagrees with the Coalition’s push to prohibit the collection of behavioral data from adolescents between the age of 13 and 18. These adolescents have an independent right to access information and participate in activities online. CDT is concerned that prohibitions on collection of information will prompt content providers to block adolescents from their sites altogether (or at least attempt to require parental consent), thus interfering with the right of adolescents to find valuable information and communicate with others.

4. Merged Data

CDT Recommendation: We join the FTC in resisting the categorization of information as either non-PII or PII. However, under a paradigm that continues to recognize this division, we believe that if a consumer is informed that only non-PII is being collected but later an entity wants to merge this non-PII with PII, then the entity must obtain opt-in consent from the consumer before the data merger can occur.

Recognizing that material changes in the use of collected data nullifies the consent (implicit or explicit) supposedly obtained from consumers at the time of collection, both the IAB and the NAI detail mechanisms for obtaining additional consent when such changes occur. For example, both guidelines recognize it is a material change if a company that had informed consumers that it was only collecting non-PII later wants to merge this information with PII. Before doing the merge, the company must obtain opt-in consent from consumers.

5. Behavioral Trackers Who Collect and Use All or Substantially All Internet Traffic Content

CDT Recommendation: Echoing our position in the Transparency section of this report, CDT believes all behavioral trackers who collect and use all or substantially all Internet traffic content should offer an opt-in screen that includes a clear, comprehensive description of the types of data that will be collected, how data will be used and transferred, and how consumers can access the profiles being built about them. After

69 NAI Principles at 9; IAB Principles at 13-14; Legislative Primer at 4.

70 See NAI Principles at 9; IAB Principles at 16-17.

71 Legislative Primer at 4.

72 IAB Principles at 39; NAI Principles at 9.
consumers affirmatively opt in to data collection, an unavoidable notification screen should affirm that they have indeed consented to data collection and provide instructions for how to rescind consent. These behavioral trackers should include ongoing notice about data collection practices and a mechanism for revoking consent.

Any company that collects consumer information needs to have direct opt-in consent from one main party (either the individual or the Web site that is visited) and opt-out consent for the other. Network advertisers currently obtain consent from the publishers, but we are not satisfied with their opt-out consent mechanism. On the other hand, ISPs, toolbars or software that collect and use all or substantially all Internet traffic content would need to either get opt-in consent from every publisher or from the user directly to then allow at least opt-out consent to the other party involved.

At least three specific standards should be applied to behavioral trackers who collect all or substantially all Internet traffic content in order to target individuals: (1) unavoidable notice and affirmative, express opt-in consent, (2) ongoing notice, and (3) revocable consent. However, the burden is on those who wish to move forward with such a model to demonstrate that these standards can work in this context.

The IAB takes an encouraging step by including a distinct mechanism for control over data collected by these entities that collect all or substantially all Internet traffic content: these so-called “Service Providers” must “obtain the consent of users before engaging in online behavioral advertising.”\(^{73}\) We applaud the IAB for holding such data collectors to the higher standard of opt-in consent, and we look to the NAI, Privacy Group Coalition, and the FTC to follow the IAB’s lead in recognizing that ISPs, toolbars, and software that are engaged in behavioral advertising need to be appropriately regulated. The IAB has yet to implement these consent mechanisms, but has promised to do so by the end of 2009. CDT will be carefully evaluating the implementation process and we urge the FTC to do so as well.

B. “Mechanisms for Appropriate Access, Correction, and Redress”

CDT Recommendation: Much as consumers can access their credit reports, they should be able to access data that is being collected about them and the profiles being constructed in connection with behavioral advertising. Data access is integral to other FIPs. It provides the basis for an individual’s control over his or her online identity, including the right to seek corrections. Data access is also necessary to hold advertisers accountable for data quality and collection practices.

We agree with the Privacy Group Coalition’s position on consumer access and redress:

An individual should have the right: (1) to obtain from a behavioral tracker, or otherwise, confirmation of whether or not the behavioral tracker has data relating to him; (2) to have communicated to him data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable

---

\(^{73}\) IAB Principles at 3.
manner; and in a form that is readily intelligible to him; (3) to be given reasons if a request under subparagraphs (1) and (2) is denied, and to be able to challenge such denial; and (4) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.\(^{74}\)

Moreover, consumers should have an avenue through which they may have any or all data collected about them erased. This requirement is particularly important in an ecosystem with limited opportunities to opt out of data collection.

In addition to notice and consent, the FIP principle of “Individual Participation” also has a separate element that is often forgotten: the right of individuals to access data about themselves. CDT is pleased to see that the Privacy Group Coalition has addressed the principle of Individual Participation in a manner that includes consumers’ access to the data that has been collected about them. Consumer access aligns with consumer expectations: Sixty-nine percent of Americans would like to see a law giving them the right to access all of the information a Web site has collected about them.\(^{75}\)

The NAI also recommends a right of access for consumers, though the depth and breadth of that right is far more limited than in the Privacy Group Coalition’s guidelines:

Members shall provide consumers with reasonable access to PII, and other information that is associated with PII, retained by the member for [Behavioral Advertising] purposes.\(^{76}\)

So far, Google and BlueKai have set the standard for access to profile data. These companies offer a page that allows the user to see the categories that have been associated with that user for targeting and allows the user to edit the profile.\(^{77}\) Google’s Ad Preferences page, shown below, also shows users information about the cookie that Google is using to track them. Google also provides a prominent button that opted-in users can click to withdraw their consent.

\(^{74}\) Legislative Primer at 9-10.


\(^{76}\) NAI Principles at 9.

This type of tool also helps address the sensitive data issue in the following way: If companies must disclose the categories used to target, that will discourage them from targeting on the basis of categories that will concern users.

CDT urges all ad networks to offer such a tool. Moreover, we urge the self-regulatory bodies to work to standardize such tools so that users do not have to struggle to understand 30 or more different profiles when they make the decision to edit their profiles.

While the tools such as those offered by Google and BlueKai are an important step forward, they do not offer full access in that they do not show the consumer the underlying data on which the profile is based – they show the inferences drawn from the...
data, but they do not show what data is being collected and retained, where it was collected or what partners, if any, it is being shared with.\textsuperscript{78}

\section*{V. Purpose Specification}

\textit{Companies should specifically articulate the purpose or purposes for which data is intended to be used.}

\textbf{CDT Recommendation:} \textit{Companies should articulate the precise purpose or purposes for which collected data will be used. These statements should be specific and binding; if data will be used for reasons not detailed in the disclosure, then this amounts to a “material change” and consumers must provide affirmative consent (opt-in) before data can be used in these new ways.}

The Purpose Specification principle is a key element of FIPs, for the limitations outlined in other principles – like Data Minimization and Use Limitation – are tied to the purpose for which the data was first collected. Of the four frameworks analyzed in this report, only the FTC fails to address purpose specification in any significant way. This is particularly disappointing, as companies look to the FTC to define the terms of the discussion on behavioral advertising. We urge the FTC to include purpose specification in any future guidance as an important part of any privacy framework.

Although the FTC does not emphasize purpose specification, the IAB, NAI, and Privacy Group Coalition all address this FIP principle, albeit in different ways. The IAB, NAI, and Privacy Group Coalition each provide that notices or disclosures pertaining to behavioral advertising should describe the types of data collected and how data will be used, although the IAB specifically acknowledges that data collected for behavioral advertising purposes may also be used for other (non-specified) purposes.\textsuperscript{79} The NAI, by contrast, further emphasizes that “\textit{[m]embers directly engaging in \textit{Online Behavioral Advertising} shall only use, or allow use of, \textit{Online Behavioral Advertising} segments for Marketing Purposes.}”\textsuperscript{80}

\textsuperscript{78} It is CDT’s understanding that when designing the Ads Preference Manager, Google considered showing the underlying base data and deliberately decided not to because of the privacy concerns raised by shared computers.

\textsuperscript{79} IAB Principles at 37. “It is similar to the provisions in the 2002 DoubleClick agreement with state attorneys general insofar as it recognizes that data used for Online Behavioral Advertising purposes may also be used for other purposes[.]” The IAB does, however, reference purpose specification with respect to data shared by non-traditional entities. See IAB Principles at 15-16 (“\textit{[non-affiliates with which data is shared] will not attempt to re-construct the data and will use or disclose the anonymized data only for purposes of Online Behavioral Advertising or other uses as specified to users.}”).

\textsuperscript{80} NAI Principles at 9. “Marketing Purposes includes any activity undertaken to collect, aggregate, analyze, maintain, update, or sell information in order to tailor content or services that allows or induces consumers to take action to purchase, rent, or exchange products, property or services, to solicit a charitable donation, to utilize market research or market surveys, or to provide verification services to marketers. Certain non-marketing uses of OBA segments may already be restricted by law.” \textit{id. at 6.}
VI. Data Minimization

Only personal information relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as is necessary to fulfill a specified purpose.

A. Reducing Data Collection

CDT Recommendation: Only data directly relevant and necessary to a specified purpose should be collected. Minimizing the collection of consumer data can significantly reduce the privacy risks associated with online consumer profiling.

Data minimization plays a unique role within any comprehensive set of FIPs, and its importance needs to be re-emphasized.

We are disappointed that neither the FTC nor the trade associations specifically addressed data minimization. In contrast, the Privacy Group Coalition rightly addresses data minimization. Under the principles enunciated in the Legislative Primer, (1) the collection of personal and behavioral data “should be relevant to the purposes for which they are to be used;” (2) sensitive data should not be collected at all; and (3) “[w]ebsites should only initially collect and use data from consumers for a 24-hour period . . . [a]ny subsequent use or collection of non-sensitive consumer data must have the affirmative consent of the individual user.”

Although CDT does not believe an absolute prohibition against collecting sensitive data is necessary (a well-constructed opt-in mechanism would be sufficient) and is concerned that a 24-hour automatic opt-out trigger for other data collection may not be a workable solution, we are encouraged to see a recognition of data minimization as an integral part of any privacy framework.

Also, we applaud the Privacy Group Coalition for opening a debate on how much data is enough. Clearly, the collection of irrelevant data and the accumulation of data after it is no longer useful presents some of the greatest privacy risks to consumers. At the same time, recent research suggests that, for marketing purposes, data no more than 24 hours old is by far the most valuable. Nevertheless, we see the Privacy Group Coalition’s recommendation of an automatic purge that is triggered 24 hours after data collection commences as difficult, if not impossible to implement. CDT feels that consumers should have the opportunity for immediate opt-out. At the same time, as we discuss in the next section, CDT believes that it is necessary to begin discussing appropriate time frames for purging data.

81 Legislative Primer at 4, 8.

B. Data Retention Limits

CDT Recommendation: Data retention should be tied to the purpose for which the data was collected. This will help ensure that the data is kept only as long as necessary to complete the task for which it was collected and thus better guard against unanticipated uses.

CDT continues to believe that the FTC’s Limited Data Retention principle – “companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need” – is inadequate.\(^83\) The correct formulation of the FIP principle is that data should be retained for no longer than necessary to fulfill the purpose specified at the time it was collected, unless the consumer provides explicit consent to additional uses. The FTC’s version of the principle does not guard against unanticipated uses because data retention is not tied to the purpose for which the data was collected in the first place.

The same problem is found in both the NAI and IAB principles.\(^84\) In its response to public comments, the NAI claims that tying data retention to purpose specification is inappropriate because “consumers should be allowed to consent to secondary uses of data as circumstances change.”\(^85\) If this statement truly represents the philosophy behind NAI’s data retention principle, then the NAI should also commit to informed user consent for secondary uses.

On the other hand, the Privacy Group Coalition proposes a significant time limit on data retention in its Legislative Primer. Under the Coalition’s suggested framework, consent for the collection of information for behavioral targeting purposes would expire after three months, unless revoked earlier, and then the information collected must be deleted.\(^86\) This appears to mirror the change Yahoo! recently made to its data retention policy – Yahoo! now anonymizes user log data after three months.\(^87\) Yahoo!’s decision was based on its determination that the purpose for which the data was initially collected would not be served by data more than three months old. Three months might be a suitable retention limit for some data; the research showing that the data most relevant for marketing purposes is a mere 24 hours suggests that shorter periods may be appropriate for marketing data.

---

\(^83\) Staff Report at 47.

\(^84\) NAI Principles at 10 (members shall retain data collected for OBA, multi-site advertising and ad delivery & reporting “only as long as necessary to fulfill a legitimate business need, or as required by law”); IAB Principles at 15 (“Entities should retain data that is collected and used for Online Behavioral Advertising only as long as necessary to fulfill a legitimate business need, or as required by law”).


\(^86\) Legislative Primer at 7 (“Any consent for the collection of information for behavioral targeting purposes must be recent (e.g., within three months) and revocable. Once consent has expired or been revoked, information collected with consent must be deleted promptly”).

VII. Use Limitation

Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.

A. Secondary Uses of Data

CDT Recommendation: Personal information should only be shared for a purpose compatible with the purpose for which it was collected and only if such sharing was explicitly mentioned in the disclosure. The use of behavioral advertising data for secondary purposes needs to be further investigated and the FTC should seek additional information specifically on this topic. Secondary uses can include sharing or selling behavioral data, or using it for price discrimination or to make credit or insurance decisions. The practice raises serious concerns and CDT believes that an FTC investigation will find practices that are hidden from the public and that are entirely unexpected by average Internet users.

Until it is shown that there are legitimate reasons that are directly beneficial to consumers for secondary uses of data, CDT believes that all secondary uses should be prohibited absent explicit, affirmative consumer consent. The burden is on industry to prove that secondary uses are warranted and to get these uses approved.

The FTC’s principles do not directly address the use of tracking data for purposes other than behavioral advertising. However, the FTC explicitly notes that secondary use protections are indirectly built into its guidelines and that the principles pertaining to notice and choice may provide adequate safeguards. The FTC also suggests that a secondary use may “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 [i.e. the secondary use].” Nevertheless, the FTC recognizes that the issue merits additional consideration and dialogue. CDT agrees that additional efforts are needed here and continues to recommend that the FTC seek more information specifically on this topic, whether through a workshop or an additional written proceeding.

Like the FTC, the NAI has not directly confronted the secondary use issue and instead rely on other principles, such as transparency, purpose specification and individual participation (or consent), to protect consumers from secondary uses of data. The IAB has only addressed secondary uses of data collected by those entities that collect all or substantially all data about consumers’ online activities. These so-called “Service Providers” must obtain “satisfactory written assurance that [non-affiliates with which data is shared] will not attempt to re-construct the data and will use or disclose the anonymized data only for purposes of Online Behavioral Advertising or other uses as specified to users. This assurance is considered met if a non-Affiliate does not have any independent right to use the data for its own purposes under a written contract.”

88 Staff Report at 45 n.78.
89 IAB Principles at 15-16.
Only the Privacy Group Coalition addresses the secondary use issue head on for all types of data collection. The Coalition specifically follows the most recent definition of the FIP Use Limitation principle and would prohibit the use of behavioral targeting data “in any way other than for the advertising purposes for which it was collected.”

CDT believes that sharing or selling behavioral data, or using it for price discrimination or to make credit or insurance decisions, is a serious concern and often directly harmful to consumers. At this point it seems that only an investigation from an agency with subpoena power, such as the FTC or state attorneys general, will turn up the information necessary to have a detailed understanding of these practices.

B. Transferring Behavioral Data

CDT Recommendation: All transfers of behavioral data, whether to affiliate or nonaffiliate entities, should be transparent and specified in advance to consumers. When not clearly specified in advance, a new use (i.e., transfer) of this data should be considered a material change to a privacy policy.

The transfer of behavioral data presents an additional concern. CDT generally agrees with the Privacy Group Coalition’s treatment of this issue. The Coalition recommends that “[p]ersonal and behavioral data should not be disclosed, made available or otherwise used for purposes other than those specified in advance except: a) with the consent of the individual; or b) by the authority of law.”

The FTC does not specifically address data transfers, and the NAI and IAB only address the subject in their discussions of disclosures.

For example, under the IAB framework, disclosures must include information about whether data will be transferred to non-affiliates for online behavioral advertising purposes. However, no explanation or disclosure needs to be provided with regard to the transfer of behavioral data to affiliate entities, which is a cause for concern. And while users must be able to exercise control over whether information about them can be collected, used or transferred for the purposes of online behavioral advertising, the IAB principles do not seem to limit how data could be transferred for other purposes that “fulfill a legitimate business need.”

---

90 Legislative Primer at 8. The Coalition specifically mentions the use of data for any credit, employment, insurance, or governmental purpose or for redlining. Under the Coalition’s use limitation principle, “personal and behavioral data should not be disclosed, made available or otherwise used for purposes other than those specified in advance except: a) with the consent of the individual; or b) by the authority of law.” Id.

91 See Legislative Primer at 5.

92 IAB Principles at 12.

93 IAB Principles at 37.
In contrast, the IAB principles do require that “Service Providers,” such as ISPs, toolbars, and software that collect all or substantially all information about consumers’ online activities offer extensive controls to protect behavioral data they collect and then transfer to a non-affiliate.\textsuperscript{94} We would prefer to see these controls required for transfers to affiliates as well when the transfer is not related to the original purpose of the collection.

**VIII. Data Quality and Integrity**

*Companies should, to the extent practicable, ensure that data is accurate, relevant, timely and complete.*

**CDT Recommendation:** *Companies should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Consumer access is the best mechanism for ensuring data quality and integrity.*

Unfortunately, the FTC fails to provide any guidance in outlining mechanisms for ensuring data quality and integrity. The IAB, like the FTC, does not specifically address this issue. The NAI, on the other hand, requires members to “make reasonable efforts to ensure that they are obtaining data . . . from reliable sources.”\textsuperscript{95} While this represents a step in the right direction for data quality and integrity, “reliable sources” is not enough. Clearly, the most efficient means to ensure data quality is to engage the user. CDT encourages NAI members to provide consumers both reasonable access to data and also an efficient procedure to challenge and correct data, as suggested by the Privacy Group Coalition.\textsuperscript{96}

**IX. Security**

*Companies should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

**CDT Recommendation:** *Proper implementation of the FTC’s security guidelines will sufficiently protect consumer data.*

\textsuperscript{94} For example, service providers must “…take reasonable steps to protect the non-identifiable nature of data if it is distributed to non-Affiliates including not disclosing the algorithm or other mechanism used for anonymizing or randomizing the data, and obtaining satisfactory written assurance that such entities will not attempt to re-construct the data and will use or disclose anonymized data only for purposes of Online Behavioral Advertising or other uses as specified to users.” Reasonable steps must also be taken to ensure that any non-Affiliate to which data is transferred will also require any other non-Affiliate given the data to respect the restrictions. \textit{id.} at 15-16.

\textsuperscript{95} NAI Principles at 10.

\textsuperscript{96} See Legislative Primer at 5, 9-10 (“An individual should have the right: a) to obtain from a behavioral tracker, or otherwise, confirmation of whether or not the behavioral tracker has data relating to him; b) to have communicated to him data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.”).
In the absence of data security, all of the other FIPs become meaningless, for once data is leaked any promises about its uses become irrelevant. For many consumers, this is their worst nightmare.

All four frameworks recognize the importance of data security and require that companies that collect and store behavioral advertising data must provide reasonable safeguards for that data. Both the NAI and the IAB’s standards track those promulgated by the FTC. The FTC guidelines state:

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.

The IAB and Privacy Group Coalition additionally articulate the type of data safeguards necessary: physical, electronic, and administrative. The IAB discusses in greater depth and detail the security standards for data collected by “Service Providers,” entities like ISPs, toolbars, and certain software downloads that track all or substantially all of Internet users’ online activities. In addition to requiring that service providers “alter, anonymize, or randomize . . . any PII or unique identifier in order to prevent the data from being reconstructed into its original form in the ordinary course of business,” the IAB principles propose measures for third parties (to whom data is transferred) to take in order to assure that they are also properly securing the data.

X. Accountability and Auditing

*Companies should be accountable for complying with these principles, providing training to all employees and contractors who use personal information and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

---

97 NAI Principles at 10; IAB Principles at 36.
98 Staff Report at 46-47.
99 IAB Principles at 36; Legislative Primer at 9.
100 IAB Principles at 37-38 ("Finally, an entity, when acting as a Service Provider, should take steps to safeguard the data that is distributed. One example is not disclosing to non-Affiliates the algorithm or other mechanism used for coding the data. Another example is obtaining satisfactory written assurance from the recipients of such data that: (i) they will not attempt to identify the data; (ii) they will use or disclose the data only for purposes of Online Behavioral Advertising or other approved uses such as content organization; and (iii) they will ensure that any additional entities to which they disclose the data (e.g., subcontractors) agree to the same restrictions and conditions to which they have agreed. If a non-Affiliate does not have any independent right to use the data under written contracts, the written assurances in this subsection are considered to have been satisfied.").
A. Compliance with the Principles

**CDT Recommendation:** CDT remains skeptical of any self-regulatory approach not girded by legislation and FTC enforcement. We encourage the FTC to articulate benchmarks that will allow both the Commission and outside observers to evaluate the efficacy of self-regulation. Without such metrics, it will be difficult to judge whether industry principles are working to the benefit of consumers. Benchmarks will also provide a rubric for deciding when the various guidelines are in need of updating. Compliance reviews should be conducted by an independent third party and the results should be made public.

The FTC Principles provide guidance for industry self-regulatory programs; companies are not legally required to abide by the FTC Principles except where FTC law otherwise mandates the same principle. The FTC does have the power to initiate an investigation of unfair or deceptive practices, including violations of promises to adhere to self-regulatory principles. However, even the FTC recognizes the limits of its proposed Principles – in the staff report, it reminds companies that “self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences.”\(^{101}\) While some progress has been made through industry’s self-regulatory efforts, it nevertheless remains abundantly clear that self-regulation alone will not adequately protect consumer privacy.

The NAI has taken some positive steps in its compliance program – such as providing for attestation reviews, a consumer compliant process, the threat of sanctions (i.e., membership suspension or referring the matter to the FTC) and public annual reporting.\(^{102}\) But while NAI members must contractually require third parties to adhere to applicable provisions of the NAI Code, the Code only directly applies to companies that voluntarily join the initiative. In addition, although the NAI has done a good job of picking up new members, it cannot compel companies to join; the current membership is still missing behavioral advertising firms, including some engaging in questionable practices.\(^{103}\)

Furthermore, the NAI plan to conduct member compliance reviews in-house for the foreseeable future is problematic.\(^{104}\) CDT continues to believe that employing some kind of third party – unaffiliated with the NAI or any of its members – to conduct compliance reviews would create more public trust in the accountability process than having the NAI itself act as auditor.

---

\(^{101}\) Staff Report at 47.


\(^{104}\) See NAI Response at 45.
The Privacy Group Coalition agrees and recommends requiring a behavioral advertiser to “conduct an independent audit of its operations” and make the results public.\(^\text{105}\) As an additional auditing check on company compliance, the Coalition proposes establishing a Behavioral Tracker Registry to be governed by the FTC.\(^\text{106}\) CDT is encouraged by this idea and helped develop the Do Not Track proposal, a precursor to this type of approach.\(^\text{107}\) Absent strict compliance with FIPs, these tools will become all the more necessary.

The Coalition is also the only entity to recommend privacy training for all appropriate staff on an annual basis,\(^\text{108}\) as is specifically outlined in the Accountability and Auditing FIP principle.

Unlike the NAI and Privacy Group Coalition, the IAB only vaguely discusses accountability mechanisms or “programs” to be put in place. While the Direct Marketing Association and the Council of Better Business Bureaus have indicated a willingness to incorporate the IAB Principles as part of their self-regulatory process, programs will not be in place until, at the earliest, the beginning of 2010. It is also unclear how these accountability programs will effectively police entities engaged in behavioral advertising. Although the IAB framework does provide for some form of public reporting of instances of non-compliance, we remain deeply skeptical of the IAB Accountability principle without a program in place.

\[ B. \quad \text{Redress} \]

**CDT Recommendation:** *There must be meaningful consequences for failure to comply with FIPs.*

Without redress, companies will have little incentive to put the interests of consumers above the 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.

The NAI and IAB self-regulatory frameworks’ rely heavily on consumer complaints, but they do not provide many details and they are somewhat limited in their discussion of the remedies that should be available. The Privacy Group Coalition’s legislative framework goes much further. For example, while the NAI Code calls for members to respond to consumer complaints “within a reasonable period of time,” the Coalition demands that a behavioral targeter provide a “prompt” response to consumer complaints – within 30 days.\(^\text{109}\) More significant, under the Coalition’s approach federal and state agencies

\(^{105}\) Legislative Primer at 11.

\(^{106}\) See id. at 10-11.

\(^{107}\) See Pam Dixon et al., *Consumer Rights and Protections in the Behavioral Advertising Sector* (Oct. 2007), http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf. The Do Not Track proposal is one idea that CDT believes can work, but ultimately we want some kind of policy that follows this proposal’s underlying principles.

\(^{108}\) Id. at 11.

\(^{109}\) NAI Principles at 11; Legislative Primer at 10.
could bring enforcement actions on behalf of consumers for violations. Moreover, the Coalition recommends that “consumers aggrieved by behavioral targeting activities that violate the law or a published policy should have the right of private action that allows for the awarding of liquidated damages, attorney fees, and costs for successful plaintiffs.”

Although the NAI and IAB do not provide remedies for consumers, they do identify potential sanctions for members that violate their respective Principles. The NAI Compliance Program outlines the following process: “Based on a conclusive finding of non-compliance and failure to remedy the defect by the NAI Board, the NAI Board may suspend the member, publicly revoking its right to represent NAI membership, and referring the matter to the Federal Trade Commission’s consumer protection division.”

Similarly, the IAB enforcement “programs” would “refer entities that do not correct violations to the appropriate government agencies.” While these practices, when fully implemented, represent important steps forward, now is the time for a baseline federal privacy law and increased regulatory oversight by the FTC emphasizing the importance of the FIP principles we have discussed in this report.

XI. Conclusion

For the reasons outlined under each principle, while we encourage more robust self-regulatory efforts based on a comprehensive FIPs model, we continue to have doubts that self-regulatory frameworks can adequately protect consumer privacy when they are not girded by legal standards and more direct oversight from the FTC. Consumers will be best served by a system in which self-regulation and legislation work in concert.

The online advertising industry has yet to live up to the self-regulatory principles they have promised.

The time for action is now. The Internet is becoming the primary source for all information supported by advertising, and it is imperative that policy in this area is developed with strong protections for consumers.

As online behavioral advertising becomes increasingly complex and data collection becomes more pervasive, Congress and the FTC – via broader rulemaking authority – must step in to ensure that consumer interests are fully protected. A comprehensive online and offline privacy bill should offer the ability to specifically regulate in this space.

---

110 Id. at 10.

111 NAI Compliance Program Overview.