

Online Behavioral Advertising: Industry's Current Self-Regulatory Framework Is Necessary, But Still Insufficient On Its Own To Protect Consumers

December 9, 2009

Tags: Array

Supporting Documents

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts [here](#):

- 1) [CDT Releases Online Behavioral Advertising Report](#)
- 2) [Scope of Regulatory Frameworks](#)
- 3) [CDT Recommendations for Improving Consumer Privacy Protections](#)

1) **CDT Releases Online Behavioral Advertising Report**

CDT released a report in December 2009 analyzing the current behavioral advertising frameworks of the Federal Trade Commission (FTC), Network Advertising Initiative (NAI), Interactive Advertising Bureau (IAB) and Privacy Group Coalition (none of which had been comprehensively implemented as of the paper's release) and provides CDT's specific recommendations for protecting consumers in this space.

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.

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 FTC 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.

[CDT Online Behavioral Advertising Report](#) [1]: Industry's Current Self-Regulatory Framework Is Necessary, But Still Insufficient On Its Own To Protect Consumers

[Federal Trade Commission Staff Report](#) [2], Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting & Technology

2) **Scope of Regulatory Frameworks**

The definition of online 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.

The FTC's proposed self-regulatory principles apply broadly to companies engaged in online behavioral advertising. 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 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.

Further, 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. 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 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. 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.

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.

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.” This is a step in the right direction.

Regulation must also protect any type of data that can be used to identify, contact, or locate an individual. 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 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.

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.

[Federal Trade Commission Staff Report](#), [2] Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting & Technology

Network Advertising Initiative, 2008 NAI Principles: The Network Advertising Initiative's [Self-Regulatory Code of Conduct](#) [3]

Interactive Advertising Bureau, [Self-Regulatory Principles](#) [4] for Online Behavioral Advertising

[Legislative Primer September 2009](#) [5], Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of: Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group and The World Privacy Forum

3) **CDT Recommendations for Improving Consumer Privacy Protections**

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. 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. The extra level of protection afforded sensitive data should be granted, at a minimum, to: (1) Information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information of an individual; (2) Financial information about an individual; (3) Information about an individual's sexual behavior or sexual orientation; (4) Social Security Numbers or any other government-issued identifiers; (5) Insurance plan numbers; and (6) Information indicating the precise geographic location of an individual when he or she accesses the Internet.
- 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

- The collection and aggregation of consumer data should be minimized.

- Data retention should be tied to the purpose for which the data was collected.

Use Limitation

- 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.
- All transfers of behavioral data, whether to affiliate or non-affiliate entities, should be transparent and specified in advance to consumers.
- 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

- Consumer profile access is the best mechanism for ensuring data quality and integrity.

Security

- Proper implementation of the FTC's security guidelines will sufficiently protect consumer data.

Accountability and Auditing

- Any self-regulatory approach should be 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.
- Compliance reviews must be public and conducted by independent third parties.
- There must be meaningful consequences for failure to comply with these FIP principles.

For a more detailed analysis of these recommendations, please see our [report](#) [1].

- [FTC](#)
- [behavioral advertising](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://www.cdt.org/policy/online-behavioral-advertising-industry%E2%80%99s-current-self-regulatory-framework-necessary-still-in>

Links:

[1] <http://www.cdt.org/report/online-behavioral-advertising-industrys-current-self-regulatory-framework-necessary-still-ins>

[2] <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>

[3] http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf

[4] <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>

[5] http://www.uspirg.org/uploads/2S/DP/2SDPw9Zo08rEL_0XahnCmg/OnlinePrivacyLEGPRIMERSEPT0



9.pdf