CENTER FOR DEMOCRACY & TECHNOLOGY

Keeping the Internet Open, Innovative and Free

Comments Regarding the NAI Principles 2008: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising

June 12, 2008

Introduction

The Center for Democracy & Technology (CDT) appreciates the opportunity to comment on the NAI Principles 2008: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising.[1] We are pleased that the NAI has chosen to incorporate input from commenters in its revision of the principles, as we believe this will result in a better self-regulatory code for the network advertising industry.

We welcomed the original NAI principles when they were issued in 2000 as an important first step, although we saw room for improvement even in the initial version. We had hoped that the NAI would regularly update its principles, and, in recent years, as technological evolution has accelerated and consolidation among online advertising companies has taken hold, we have urged the NAI to revisit its principles both to resolve the issues present in the original version and to address emerging issues in the marketplace. Thus, we are very pleased that the NAI has finally undertaken to update its principles. Although it remains uncertain how the NAI principles will interact with the outcome of the FTC's work on its proposed guidelines for behavioral advertising self-regulation,[2] the NAI is still the only self-regulatory framework that addresses behavioral advertising specifically, making revision of the principles all the more important.

Our comments are divided into four parts:

- Part I recommends that the NAI guidelines expressly address advertising networks' use of Internet traffic content from Internet Service Providers (ISPs) for behavioral advertising. We suggest that ISPs engaged in such practices be

[1] Network Advertising Initiative, *NAI Principles 2008: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising* (Apr. 2008), http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf ("NAI Principles 2008").

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

required to provide unavoidable notice and obtain affirmative, express opt-in consent, that ISPs should display ongoing notice of these practices, and that when consumers revoke their consent their Internet traffic data should no longer be collected.

- Part II discusses our concern with the NAI's segmented approach to sensitive information, and recommends a more uniform approach.

- Part III suggests a stronger standard for the NAI's opt-out provision, which would do more to put consumers in control of the data collected about them for behavioral advertising purposes.

- Part IV provides a section-by-section analysis of the principles, covering issues we do not address in parts I, II and III.

We continue to have concerns about the effectiveness of the self-regulatory principles due to the limited scope of the membership of NAI, which is missing numerous behavioral advertising firms, including some key industry players. However, we have limited our comments here to the substance of the NAI's draft principles.

I. The NAI Should Address Behavioral Advertising Using Internet Traffic Content From ISPs

CDT believes the NAI guidelines should expressly address advertising networks' use of Internet traffic content from Internet Service Providers (ISPs) for behavioral advertising. Behavioral advertising networks that access and inspect the content of consumer traffic at the ISP level have gained significant attention in recent months.[3] In this new model, an advertising network strikes a deal with an ISP that allows the network to receive the contents of the individual Web traffic streams of each of the ISP's customers. The advertising network analyzes the content of the traffic in order to create a record of the individual's online behaviors and interests. As customers of the ISP surf the Web and visit sites where the advertising network has purchased advertising space, they see ads targeted based on their previous Internet behavior. While the model that has been described so far involves an ISP contracting with a third party to operate such a behavioral advertising network, it would also be possible for ISPs to do the traffic content inspection, categorization, and ad delivery themselves.

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

This new model already falls within the NAI's proposed definition of "third-party online behavioral advertising," (OBA)[4] but the draft principles do not address the need for heightened protection that we believe this model requires. There are three specific standards that we think should be applied to behavioral advertising networks' use of Internet traffic content from ISPs: 1) unavoidable notice and affirmative, express opt-in consent, 2) ongoing notice on ISP Web sites, and 3) revocable consent for data collection.

Unavoidable Notice and Affirmative, Express Opt-In Consent

Advertising networks that make use of Internet traffic content may potentially gain access to all or substantially all of an individual's Web traffic as it traverses the ISP's infrastructure, including traffic to all political, religious, and other non-commercial sites. A traditional ad network generally can collect data about a user's behavior only when the user visits the Web sites participating in that particular ad network. While today's ad networks may be large, they still do not provide the opportunity to collect information about an individual's online activities as comprehensively as in the ISP model, particularly with respect to activities involving non-commercial content.

The use of Internet traffic content for behavioral advertising defies user expectations. Absent clear notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications. Finding out that a middleman sits between consumers and the Web sites they visit would likely come as a huge surprise to most Internet users.

In part, this expectation of privacy derives from the laws that protect consumers' electronic communications from interception and disclosure. The Electronic Communications Privacy Act (ECPA) and its amendments to the Wiretap Act prohibit the interception and disclosure of electronic communications – including Internet traffic content – without consent.[5] Although exceptions to this rule exist, it is our understanding that none of them apply to the interception or disclosure of Internet traffic content for behavioral advertising purposes. While the privacy risks of this behavioral advertising model grow with the amount of Internet traffic content collected, even the interception and disclosure of small amounts of Internet traffic content are prohibited by this rule.

Accordingly, we believe that the use of Internet traffic content from ISPs for behavioral advertising purposes requires unavoidable notice and affirmative, express opt-in consent. Consumers should be confronted with an unmistakable notice before the data collection begins. The notice should be written clearly in plain language such that it is easily understandable. Consumers should be required to affirmatively agree to the collection and use of their Internet traffic content before it can be used for behavioral advertising purposes. If they do not agree, their Internet traffic content should not be collected.

[4] NAI Principles 2008 at 4.

[5] See 18 U.S.C. 2511.

The only way we envision this notice being delivered is through the ISP, since the ISP – not the advertising network – is the company that consumers have a direct relationship with. ISPs are not currently members of NAI. Nevertheless, NAI members should commit, though the self-regulatory principles, not to engage in any activity involving use of Internet traffic content obtained from or with the cooperation of an ISP unless the ISP is giving its customers unavoidable notice of the practice and is obtaining their affirmative, express opt-in consent. The NAI could institute these standards by adding provisions to its Notice principle (Section III(2)) and its Choice principle (Section III(3)). The Notice principle could be augmented with an additional subsection (e) as follows:

> *e) Each member that uses Internet traffic content from an Internet Service Provider (ISP) for OBA shall provide, or require its ISP partners to provide, an unavoidable, clear, and consumer-friendly statement to explain that the consumers' Internet traffic content will be collected and used for OBA purposes.*

As the NAI's proposed definition of "opt in to OBA" (Section II(3)) already includes the concepts of "affirmative" and "express" consent, the consent standard for use of Internet traffic content could be added to the principles merely by adding the following to the Choice principle (under Section III(3)(a)):

> *v. Use of Internet traffic content from ISPs for OBA shall require a consumer's opt-in consent to OBA.*

The NAI principles include in a separate section provisions about members' compliance with applicable law,[6] and although we believe the law already requires notice and consent, these provisions in the context of Internet traffic content use for OBA are important enough to warrant specific attention in Section III. In addition, these issues should be specifically addressed because there is likely some disagreement as to exactly what the Wiretap Act requires and because the Act does not apply in jurisdictions outside the United States.

Ongoing Notice on ISP Web Sites

For the NAI to sufficiently cover behavioral advertising networks using Internet traffic content from ISPs, the ISPs involved should be required to maintain notice about the practice on their Web sites. As noted above, the ISP – not the advertising network – is the company that consumers have a direct relationship with. Therefore, the ISP is the most logical place where consumers would go to seek information about OBA conducted using their Internet traffic content after they have seen the unavoidable notice described above and made a choice about whether to participate in the behavioral advertising system.

The NAI could meet this requirement by inserting the following as Section III(2)(f):

[6] NAI Principles 2008 at 10.

e) Each member that uses Internet traffic content from an Internet Service Provider (ISP) for OBA shall require the ISP to post a clear, concise, consumer-friendly and prominent statement on its Web site describing the practice and containing the elements described in subsection (a).

This would ensure that all of the information the advertising network makes available on its own site in compliance with Section III(2)(a) – information about the types of OBA conducted, the types of data collected, how the data is used, the types of PII merged with non-PII, information about consumers' choices, and information about data retention times – would also be available from the ISP site, where consumers are more likely to find it.

Revocable Consent for Data Collection

CDT has long held that consumer control is fundamental to the continued success of the Internet. If Internet traffic content is being used for behavioral advertising, we believe consumer control means that even after consumers have opted in to the data collection, they should be able to revoke that consent at any time, at which point both the collection and the use of their Internet traffic content should cease. Otherwise, a consumer who opts in to this type of system may have no choice but to switch ISPs (if that is possible in his or her particular neighborhood) in order to stop the Internet traffic content collection. This is not an acceptable scenario – consumers should be able to control whether their Internet traffic content is intercepted and disclosed without having to change ISPs.

We believe this idea is consistent with the Wiretap Act. It seems quite clear that the Wiretap Act prohibits ISPs from intercepting, copying, and disclosing the contents of a customer's communications unless the consumer has consented (or pursuant to other exceptions not applicable here), so it is equally clear that it is impermissible to continue copying and disclosing the content after the consumer has revoked consent by opting out.[7] (The same section of the Wiretap Act prohibits third parties from using any information obtained after opt-out.)

The NAI could incorporate this provision by adding a sentence to the language we suggest above as an addition to the Choice principle (under Section III(3)(a)):

v. Use of Internet traffic content from ISPs for OBA shall require consumers' opt-in consent. Collection, use, and disclosure of consumers' Internet traffic for OBA purposes should cease if they later revoke their consent.

NAI member ad networks will likely need to work with their ISP partners in order to comply with this requirement, especially if those ISPs are not also NAI members. It should be made clear, for example, that an advertising network would be in violation of this principle if it had a non-NAI-member ISP partner that continued to disclose Internet

[7] 18 U.S.C. 2511(1).

traffic content to the advertising network even after a consumer revoked his or her consent. Thus, to comply with the principle, advertising networks would have to contractually require their ISP partners to cease intercepting and disclosing Internet traffic content when consumers revoke their consent.

When consumers revoke their consent, we would hope that behavioral advertising networks and their ISP partners would no longer use the traffic content data collected while the consumers were opted in. If this is not the case, the fact that previously collected Internet traffic content data will continue to be used should be disclosed to consumers at the time when they revoke their consent.

II. Sensitive Information Requires a Uniform Approach

What has been termed "sensitive information" in behavioral advertising discussions – data that deserves some form of heightened protection – is referred to in the NAI principles as "restricted and sensitive consumer segments." The discussion of this issue is split between two sections in the principles: a definition provided in Section II(6) and a more in-depth discussion of the issue in Addendum A: Guidelines on Restricted and Sensitive Consumer Segments.

Section II(6) – Definition of Restricted and Sensitive Consumer Segments

The definition given in Section II(6) begins as follows:

> Restricted and sensitive consumer segments include, but are not limited to:
>
> - Certain medical/health conditions; and
> - Certain personal life information.[8]

As we explain below, we disagree with the idea of assigning special protections only to certain health conditions but not others. However, should the NAI decide to retain these distinctions, we think the specific types of data that belong to restricted and sensitive consumer segments should be named explicitly in Section II(6), rather than in an addendum. As this definition stands now, it explains almost nothing to the reader, since "certain medical/health conditions" and "certain personal life information" are so generic that they could be understood to comprise almost any type of data. If the NAI pursues the path of singling out certain health and personal life data types for special protections, those data types should be listed here.

[8] NAI Principles 2008 at 5.

Addendum A: Guidelines on Restricted and Sensitive Consumer Segments

Addendum A explains in depth the NAI's approach to restricted and sensitive consumer segments. The NAI lists seven data types (divided into two groups) that, at a minimum, comprise this category:

> Certain medical/health conditions --
> A. HIV/AIDS status
> B. Sexually related conditions (e.g., sexually transmitted diseases, erectile dysfunction)
> C. Psychiatric conditions
> D. Cancer status
> E. Abortion-related
>
> Certain personal life information --
> A. Sexual behavior/orientation/identity (i.e., lesbian/gay/bisexual/transgender)
> B. Criminal victim status (e.g., rape victim status)[9]

These seven data types are referred to as "sensitive" consumer segments when they are used in conjunction with PII for behavioral advertising, and are otherwise referred to as "restricted" consumer segments.

We found this segmented approach to be misguided, confusing, and inadequate. The NAI admits that drawing the line between the data types that deserve special protections and those that do not is difficult, and we agree. However, we do not believe the NAI is in a position to judge which health conditions deserve special treatment and which do not. The NAI says in the principles themselves that "what makes one consumer personally uncomfortable may bear little relation to the privacy expectations of another consumer."[10] We believe this is especially true for health information, making it impossible for anyone – including the NAI – to judge which categories of health information make a particular consumer more uncomfortable than others.

Thus, rather than cherry-picking a handful of health conditions to be considered as restricted, the NAI should use the following broad definition of health information (which we first espoused in our comments on the proposed FTC self-regulatory principles):[11]

> *Health information is information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information.*

---

[9] NAI Principles 2008 at 12.

[10] NAI Principles 2008 at 12.

[11] FTC Comments at 24.

All information in this category should be afforded the special protections of "restricted" information (which requires opt-in consent for use in OBA) or "sensitive" information (which is prohibited for OBA purposes), as described in the NAI principles.

Even with a broader definition of health information, we believe there are several other types of data that deserve the heightened protections of the restricted and sensitive categories: financial information, Social Security Numbers or any other government-issued identifiers; insurance plan numbers; and information that describes the precise geographic location of an individual. All of these data types have been given special protections in law in the United States. Not only are they missing from the NAI's proposed "restricted" list, but they also do not appear on the NAI's much more expansive list of "potentially restricted or sensitive consumer interest segments," which includes the following:

> Age/Birth date
> Addictions (e.g., drugs, alcohol, gambling)
> Alienage or nationality
> Criminal history
> Death
> Disability
> Ethnic affiliation
> Marital status
> Philosophical beliefs
> Political affiliation or opinions
> Pregnancy
> Race identification
> Religious affiliation (or lack thereof)
> Trade union membership[12]

The other notable omissions from this list are other health conditions not already covered by the NAI's "restricted" designation.

The NAI's reasoning for paying specific attention to these categories of "potentially" restricted data is unclear to CDT. The NAI explains that while these data categories may sometimes fall into the restricted group, at other times they may not. The NAI goes on to say that "individual companies will have to make determinations" as to whether to include these data types in the restricted group.[13]

Individual companies already make these determinations – there is no need for the NAI to re-state this fact. The entire purpose of the NAI is to create uniform standards for the industry at large. Providing an incomplete list of these "potentially" restricted data types does not create any sort of uniformity, muddles the NAI's already-confusing message on restricted and sensitive information, and does nothing to help consumers understand how

[12] NAI Principles 2008 at 12.

[13] NAI Principles 2008 at 13.

their data is being used for OBA. Consumers hardly understand that multiple third parties on a given Web site are collecting and using their data – how can they be expected to understand that each of these third parties treats their criminal history, ethnic affiliation, or marital status differently?

We believe the better approach for the NAI would be to establish one set of data types it considers restricted. We also believe that the terms "restricted" and "sensitive" are confusing, because the data types are always sensitive, whether or not they are used in conjunction with PII.

Recommendations

To address all of the issues discussed above, we have the following recommendations:

- Change the definition of "restricted and sensitive consumer segments" in Section II to the following:

  6. Sensitive information

  Sensitive information consists of: information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information; information about an individual's sexual behavior, orientation, or identity (e.g., lesbian/gay/bisexual/transgender); information about criminal victim status (e.g., rape victim status); financial information; Social Security Numbers or any other government-issued identifiers; insurance plan numbers; and information that describes the precise geographic location of an individual.

- Throughout the principles, replace "restricted consumer interest segments" with "sensitive information."

- Throughout the principles, replace "sensitive consumer interest segments" with "sensitive information used in conjunction with PII."

- Eliminate the subsection of Addendum A that deals with "potentially restricted or sensitive consumer segments."

- Update the remainder of Addendum A so that it is consistent with the definition of "sensitive information" proposed above.

III. Opt-Out Choice Should Do More To Put Consumers in Control

The definition provided in Section II(4) of the principles for "opt out of OBA" is as follows:

> Opt out of OBA means that a consumer is provided an opportunity to exercise choice to disallow OBA with respect to a particular browser.[14]

This definition continues the discredited practice of allowing behavioral advertising networks to rely solely on opt-out cookies as their consumer choice mechanism. CDT was critical of the fact that NAI members began using opt-out cookies as their choice mechanism when the NAI was first formed, and we continue to be critical today.[15] The drawbacks of opt-out cookies have been well-documented: they are confusing for the majority of consumers who do not understand cookies; they are non-intuitive even for consumers who do understand cookies and are accustomed to deleting their cookies to protect their privacy; and they are susceptible to accidental deletion and file corruption.

In addition, we noted that in Section III(3)(a)(i), the discussion of the Choice principle contains the following footnote:

> Note: If a consumer elects to opt out of non-PII OBA, collection of non-PII data regarding that consumer's browser continues for non-OBA purposes, such as ad delivery and reporting.[16]

This fact is too significant to be buried in a footnote, and should instead be part of the opt-out definition. It is critically important that consumers understand what they are opting out of, and if opting out does not have any effect on data collection, that fact should be stated up front when the consumer accesses the opt-out mechanism.

To address both of these concerns, we suggest that the NAI use the following definition of "OBA opt-out mechanism" in place of its proposed definition of "opt out of OBA." This definition is based in part on language we suggested to the FTC for its proposed behavioral advertising principles:[17]

---

[14] NAI Principles 2008 at 5.

[15] *See* Stefanie Olsen, "Ad firms benefit from FTC privacy decision," *CNET News.com* (Jul. 2000), http://news.cnet.com/2100-1023-243822.html; Center for Democracy & Technology, *Applying the FTC's Spyware Principles to Behavioral Advertising: Comments of the Center for Democracy & Technology in regards to the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology*" (Oct. 2007), http://www.cdt.org/privacy/20071019CDTcomments.pdf at 8.

[16] NAI Principles 2008 at 7.

[17] Center for Democracy & Technology et al., *Comments of the Center for Democracy & Technology, Consumer Action, and Privacy Activism In Regards to the FTC Staff Statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles"* (Apr. 2008), http://www.cdt.org/privacy/20080411bt_comments.pdf at 22.

> *An OBA opt-out mechanism is a clear, easy-to-use, and accessible method that gives consumers the ability to disallow OBA with respect to a particular browser. The method should include a simple explanation of the precise effects of opting out and should clearly describe to consumers what non-OBA uses will be made of their information, notwithstanding the opt-out. A consumer's choice expressed using this method should be honored persistently until the consumer decides to alter the choice.*

Such a definition would ensure that consumers can easily find and use the opt-out mechanism, that they can review or alter their choices at any time, and that their choices to opt out persist until they decide to opt back in. It also makes certain that the information consumers need about what happens when they opt out will be available and accessible. With consumer control so central to protecting privacy online, the NAI needs this more robust opt-out standard.

IV. Section-by-Section Analysis

We provide comments below on Sections I-IV of the principles: Introduction, Terminology, OBA Requirements for NAI Members, and Procedural Matters & Enforcement.

Section I: Introduction

In the opening of its principles, the NAI claims:

> More relevant advertising creates a win-win for both consumers and companies, because consumers find more of what interests them and companies spend less on ineffective advertising.[18]

CDT is unaware of any evidence supporting the claim that behavioral advertising leads to more sales or greater brand awareness than other forms of advertising. If the NAI has concrete numbers in support of claims about behavioral advertising's effectiveness, it should publish that data in furtherance of the principle espoused in Section III(1)(b), that "members shall use best efforts, both individually and collectively, to educate consumers about behavioral advertising."[19]

[18] NAI Principles 2008 at 2.

[19] NAI Principles 2008 at 6.

Section II: Terminology

We provide comments below about the NAI's proposed definitions of online behavioral advertising (OBA), opt in to OBA, and personally identifiable information (PII). Our comments on the definition of opt out of OBA can be found in part III.

Section II(1): Third-Party Online Behavioral Advertising ("OBA")

The definition provided for online behavioral advertising (OBA) is as follows:

> OBA means any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online.[20]

Our comments on this definition pertain to: 1) ensuring that it covers behavioral advertising networks broadly, and 2) expanding the definition to include entities beyond those that "categorize likely consumer interest segments."

1) Clarifying the Broad Application of the OBA Definition

The proposed definition of OBA conflicts with the language in the introduction of the principles, where the NAI appears to contemplate a much narrower meaning of OBA. In the introduction, the NAI describes the process of online behavioral advertising in this way:

- A consumer goes on to the Internet and types a URL into their browser to visit a website.
- *Because that website has signed an agreement with an ad network to be part of its "network" of websites*, when the consumer visits the website a separate "connection" with a third party ad server is also established. . ..
- *As the consumer moves to a different website that is also part of that same "network" of websites*, the consumer's computer will again call that same third-party ad server, which will see that it has already placed a cookie and will add information to its own marketing segment file associated with that cookie.[21]

(emphasis added)

Whereas the language in the introduction describes an advertising network that has signed agreements with a network of Web sites, the definition of OBA makes no mention of such agreements or network, using the much broader description of "any process used whereby data are collected across multiple web domains." CDT believes that the NAI should govern a broad array of entities engaged in behavioral advertising – including those that collect Internet traffic content from ISPs, as discussed above – and not be limited to one particular business model in which advertising networks sign agreements

[20] NAI Principles 2008 at 4.

[21] NAI Principles 2008 at 2.

with networks of Web sites to collect data for OBA. In this respect we believe the definition of OBA proposed by the NAI takes the right tack, and that the introduction language should be clarified so as to either explicitly specify that it describes merely one behavioral advertising business model of many, or to explain the behavioral advertising process in more broad terms.

2) Going Beyond Categorizing Likely Consumer Interest Segments

The definition of OBA focuses only on processes used to "categorize likely consumer interest segments," but as this phrase is not defined in the principles, its meaning is unclear. We believe it could be interpreted in two different ways. One way would be categorizing a particular consumer's interests – for example, some sort of record would be kept about a consumer who had viewed multiple different Web sites related to sports that would indicate this interest. The other way would be grouping multiple consumers together based on their interests, so consumers who had visited sports sites would be grouped together. For the purposes of the discussion below, we will assume that the first meaning was intended, since to our understanding that is the more common model in use today.

CDT disagrees with the idea that the NAI principles should only apply to companies that use the data they collect to "categorize likely consumer interest segments." Indeed, the privacy risks that arise from behavioral advertising are not limited to the situation where data is used to categorize consumers' interests – in many cases the mere collection of the data can create threats to privacy, and there are other uses of data beyond categorization of interests that are cause for concern.

Consider, for example, an advertising network that retains a list of the top 10 domains that an individual consumer visits most frequently, and serves ads to that consumer based on this list. This practice may not necessarily constitute categorization of the consumer's interests per se, but it raises many of the same privacy questions about notice, choice, access, security, and other issues as would using the same data to categorize the consumer's interests.

To ensure that companies that collect the same kinds of data about consumers' Web activities for similar purposes are all covered by the NAI principles, we suggest the following revision to the definition of OBA, which is based on part of the language used by the FTC in its proposed definition of behavioral advertising (suggestion in italics):[22]

> OBA means any process used whereby data are collected across multiple Web domains owned or operated by different entities to *deliver advertising targeted to individual consumers' interests.*

[22] FTC Principles at 2.

Using this language or something similar will ensure that all behavioral advertising networks are covered by the NAI principles, whether or not they use the data they collect to categorize consumers' interests.

Section II(5): Personally Identifiable Information (PII)

The definition provided for personally identifiable information (PII) is as follows:

> PII means data used or intended to be used to identify, contact, or locate a person, including name, address, telephone number, or email address.[23]

This definition is largely the same as the one used in the original version of the NAI principles, albeit with the addition of the phrase "intended to be used."[24] This is a welcome addition, since it includes in the definition of PII information that in other contexts may not be considered identifiable, but whose intended use is to identify individuals for behavioral advertising purposes.

However, this definition is still limited to information "used or intended to be used" by NAI members, which leaves out information that can be used to identify, contact, or locate an individual. Under the NAI's proposed definition, a network advertiser could collect consumers' names, addresses, and even social security numbers, and that information would not be considered PII unless the network advertiser used or intended to use it to identify, contact, or locate those consumers. One could imagine a network advertiser collecting personal information in order to learn corresponding socio-economic information, for example, and in that case the NAI principles would not view such data as PII.

CDT believes this is a significant loophole in the principles, which predicate notice and choice requirements largely based on whether PII or non-PII is being used for OBA. Given the sensitive nature of PII, we believe it deserves the same level of treatment whenever it is collected, regardless of its intended use. Thus, we recommend the following revision to the definition of PII (suggestion in italics):

> PII means data *that can be used or is* intended to be used to identify, contact, or locate a person, including name, address, telephone number, or email address.

We also noted that in both Section III(2), which concerns notice, and Appendix B, which provides guidelines for notice language, the sample notice language for non-PII OBA begins with the following:

---

[23] NAI Principles 2008 at 5.

[24] Network Advertising Initiative, *Network Advertising Initiative Self-Regulatory Principles for Online Preference Marketing By Network Advertisers* (Jul. 2000), http://networkadvertising.org/pdfs/NAI_principles.pdf ("NAI Principles") at 21.

> We use third-party advertising companies to serve ads when you visit our website. Some of these companies may use information (not including your name, address, email address or telephone number) about your visits to this and other websites in order to provide advertisements about goods and services of interest to you.[25]

Although we understand that this is merely a sample of language that network advertisers could use to satisfy the NAI's disclosure standards, it seems to imply that name, address, email address, and telephone number are the only elements that comprise PII. The definition itself lists these four elements as examples of PII, but is not strictly limited to them, and we do not believe it should be limited in this way. Certainly there are other data elements – social security numbers, other assigned identifiers, IP addresses in some cases – that meet the requirements of the PII definition.

The NAI should clarify in this sample notice language that PII is not limited to these four data elements. Our suggestion is as follows (in italics):

> We use third-party advertising companies to serve ads when you visit our website. Some of these companies may use information (not including your name, address, email address, telephone number, *or other personally identifiable information*) about your visits to this and other websites in order to provide advertisements about goods and services of interest to you.

Section III: OBA Requirements for NAI Members

In the discussion below we provide comments on the proposed NAI requirements for Transparency, Notice, Choice, Use Limitations, and Transfer & Service Restrictions.

Section III(1): Transparency

Because few consumers have direct relationships with behavioral advertising networks, transparency has been and continues to be exceedingly important in this area. We are pleased that the NAI remains committed in principle to both transparency and consumer education.

A key part of the NAI's transparency mission should be to inform consumers about the choices they have with respect to behavioral advertising. The NAI itself has acknowledged that some consumers have difficulty using the opt-out cookie mechanism provided by NAI members, largely stemming from browser compatibility issues.[26] Others have conducted independent tests detailing similar problems with opt-out cookie

[25] NAI Principles 2008 at 7 and 14.

[26] Network Advertising Initiative, *Network Advertising Initiative (NAI) Written Comments for the FTC's Ehavioral Advertising Town Hall Forum* (Oct. 2007), http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf at 5.

functionality.[27] To help consumers understand these issues and how to make NAI members' opt-out mechanisms work, the NAI should provide detailed explanations of these browser configuration issues on its Web site. Although the NAI already provides links to instructions for how consumers can enable third-party cookies in their browsers, a listing of other configuration issues and instructions for how to fix them should be added. An opt-out mechanism is useless to a consumer if it does not function properly. Documenting known opt-out functionality issues should be part of the NAI's transparency efforts.

We also think that although the NAI Web site is consumer-facing and the principles themselves are directed at network advertisers, the principles should be linked directly from the NAI Web site. The original NAI principles – which still govern NAI members – were at times in the past not linked from the NAI site, which made them harder for consumer advocates, the press, and interested consumers to find.

Section III(2): Notice

Our comments on this section pertain to 1) notice on NAI members' sites, 2) notice on publisher sites, and 3) notice through Web browsers. Our comments from part I above regarding ISP notice also apply to this section of the principles.

1) Notice on NAI Members' Web Sites

Section III(2)(a) requires NAI members to post notices on their own Web sites:

> Each member shall clearly and conspicuously post notice on its website that describes its data collection and use practices.[28]

With the release of its proposed self-regulatory principles, the FTC suggested a slightly higher standard for notices regarding behavioral advertising: "clear, concise, consumer-friendly, and prominent."[29] We believe the NAI should adopt this standard in place of its notion of clear and conspicuous, as the FTC's formulation promotes greater consumer understanding. Section III(2)(a) could be revised as follows (suggestion in italics):

> Each member shall post *a clear, concise, consumer-friendly, and prominent statement* on its website that describes its data collection and use practices.

Section III(2)(a) goes on to describe what should appear in the notice: the types of OBA conducted, the types of data collected, how the data is used, the merger of PII with non-PII, an easy procedure for exercising choice, and the length of time that OBA data is

[27] Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (Nov. 2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf at 16-17.

[28] NAI Principles 2008 at 6.

[29] FTC Principles at 3.

retained. There is one additional element that would be informative for consumers and should be disclosed: the consumer's current opt-out/opt-in status. The NAI currently provides an indication of this status for each member company when consumers visit the NAI site, but we think it would be helpful for consumers to have access to their status on individual member sites as well, particularly if they are considering whether to opt out or opt in to OBA. To satisfy this requirement, the NAI could add the following to its list of required notice elements:

> *The consumer's current opt-out/opt-in status.*

2) Notice on Publisher Web Sites

Section III(2)(b) asserts that NAI members should require the publishers with which they have contracts to post notices on the publisher sites:

> Each member shall require that a publisher with which it contracts for OBA services shall clearly and conspicuously post notice, or ensure, as applicable, that such notice be made available on the website where data are collected for OBA purposes, that contains. . .[30]

We have several suggested revisions on this subsection of the Notice principle which are reflected in proposed language at the conclusion of this discussion.

First, the "clearly and conspicuously" language should be replaced with the "clear, concise, consumer-friendly and prominent" language proposed by the FTC, as with Section III(2)(a) discussed above.

Second, we are concerned that allowing members to "ensure, as applicable" that notice be made available on publisher Web sites would allow them to circumvent the notice requirement in Section III(2)(b) altogether. The NAI explained to the FTC that this phrase was inserted to accommodate NAI members wishing to deliver notice on publisher Web sites through some means other than a privacy policy.[31] But the way it is phrased implies that there are instances in which notice is not applicable at all. We believe notice is always applicable, and as such we suggest removing the "as applicable."

Third, we believe that all Web sites where NAI members collect data for OBA should be subject to the notice requirement articulated in Section III(2)(b), as opposed to only those publishers with whom NAI members have contractual relationships. This is more consistent with the FTC's proposed notice standard, which would apply to "every website where data is collected for behavioral advertising."[32]

---

[30] NAI Principles 2008 at 7.

[31] Network Advertising Initiative, *Network Advertising Initiative Written Comments in Response to Federal Trade Commission Staff's Proposed Behavioral Advertising Principles* (Apr. 2008), http://networkadvertising.org/networks/NAI_comments_FTC_BT.pdf at 21.

[32] FTC Principles at 3.

The following revision would address all of these issues (suggestions in italics):

> Each member shall require that a publisher *Web site where the member collects data for OBA purposes* shall *post a clear, concise, consumer-friendly and prominent statement (or otherwise ensure that such a statement appears)*, that contains. . .

Section II(2)(b) goes on to describe what should appear in the publisher site notice. One of these elements is "a conspicuous link to the OBA choice mechanism (e.g., opt out link) provided by the NAI member."[33] We think it would be helpful for publishers to link directly to the NAI opt-out site, in addition to or instead of linking to an individual member's opt-out mechanism. When consumers are looking for information about their choices with respect to OBA conducted by one advertising network, it would likely be useful for them to learn about which other advertising networks conduct OBA and the choices that those networks offer. The following revision would accomplish this (suggestion in italics):

> A conspicuous link to the OBA choice mechanism (e.g., opt out link) provided by the NAI member, *and/or a conspicuous link to the NAI opt-out site.*

> 3) Notice Through Web Browser Software

For all of the different kinds of notice required by the NAI principles, Web sites may not be the only suitable vehicles for disclosing behavioral advertising information. The NAI should consider promoting transparency through Web browser software as well.

What all Web sites where behavioral advertising data is collected have in common is the fact that they are displayed to consumers through Web browsers. The browser may thus be a logical place where behavioral advertising disclosures could be displayed. 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 obviously require Web sites to somehow communicate the necessary information to browser software so that the browser may display it.

We do not necessarily see disclosure through the browser as a substitute for disclosure on Web sites themselves – for some sites one option may be more appropriate than the other. However, we believe the NAI can supplement its current notice requirements by also encouraging disclosures in browser software. The NAI could insert an additional subsection (f) in the Notice principle to communicate this:

---

[33] NAI Principles 2008 at 7.

f) The notices required by this subsection may be displayed through the consumer's Web browser software instead of or in addition to display on the Web sites of NAI members, publishers, and ISPs.

Section III(3): Choice

Section III(3)(a)(iii) and Section III(3)(a)(iv) both describe types of behavioral advertising that "shall require provision of a consumer opt in mechanism."[34] While we understand that the intent of this language is to require opt-in consent, the way it is phrased may allow NAI members to provide the opt-in mechanism, but not necessarily obtain consent. We think this should be clarified so that NAI members engaging in the types of behavioral advertising described in these subsections are required to obtain consumers' opt-in consent, as opposed to being required to provide the opt-in mechanism. The revised provisions would appear as follows (suggestions in italics):

> iii. Use of PII to be merged with previously collected non-PII (retrospective merger) for OBA shall require *consumers' opt-in consent* at the time such PII is collected online or, if collected offline, first used online.
> iv. Use of restricted consumer segments for OBA shall require *consumers' opt-in consent.*

To ensure that the phrase "opt-in consent" as used above corresponds to the appropriate definition in the NAI principles, the term "opt in to OBA" as defined in Section II(3) should be changed to "opt-in consent." That way, the recommendations we make for the Choice principle above will implicate the definition of opt in that the NAI already uses.

We also noted that Section III(3)(a)(ii) requires "provision of a consumer opt out mechanism accompanied by robust notice" for use of non-PII to be merged with PII prospectively, with the explanation of robust notice provided in a footnote.[35] Because "robust notice" has a particular meaning in the context of the NAI principles, we suggest that the definition of the term be provided in Section II with the rest of the terminology definitions.

Section III(4): Use Limitations

Section III(4)(c) states that "members shall only use, or allow use of, OBA segments for marketing purposes."[36] The definition of "marketing purposes" is provided in a footnote. As with "robust notice," we suggest moving this definition to Section II with the other definitions.

---

[34] NAI Principles 2008 at 8.

[35] NAI Principles 2008 at 7.

[36] NAI Principles 2008 at 8.

We are also interested to learn whether the NAI believes that its definition of marketing purposes includes differential pricing (charging different prices to different consumers for the same good). If this is the case, we think this should be stated explicitly in the definition of marketing practices. We also suggest that if network advertisers use, intend to use, or allow others to use consumer data for differential pricing purposes, that fact should be disclosed. The NAI could achieve this by updating Section III(2)(a)(iii), which requires member companies to disclose how they will use the data they collect. In discussing the data collected by a member company, this section currently requires disclosure of "how such data will be used by the member company, including transfer, if any, of non-aggregate data to a third party."[37] This could be modified as follows (suggestion in italics):

> How such data will be used by the member company, including transfer, if any, of non-aggregate data to a third party, *and whether the member company uses, intends to use, or allows others to use the data for differential pricing purposes.*

> Section III(5): Transfer & Service Restrictions

Section III(5)(b) states:

> Members shall contractually require that any third parties to which they provide non-aggregate non-PII, to be merged with PII data possessed by that third party for OBA services, must adhere to applicable provisions of this NAI Self-Regulatory Code of Conduct. This requirement does not apply if that non-PII is itself proprietary data of the third-party publisher or advertiser.

While the first sentence refers to "any third parties," the second sentence is limited to a "third-party publisher or advertiser" that an NAI member may transfer data to. This creates some confusion about whether this provision applies to data transfers to any third parties or only third-party publishers and advertisers. There may be other kinds of third parties in this situation (data brokers, for example), and we believe this provision should apply to those third parties as well. We suggest revising the last sentence as follows (suggestion in italics):

> This requirement does not apply if that non-PII is itself proprietary data of the *third party*.

[37] NAI Principles 2008 at 6.

Section IV: Procedural Matters & Enforcement

Our only comments on this section pertain to the Accountability requirements.

Section IV(1): Accountability

The original NAI principles provided for an enforcement program that would allow a third-party enforcer to conduct audits of NAI members, including random audits and audits in response to consumer complaints.[38] The NAI Principles 2008 state that an "NAI designee" will perform compliance reviews of NAI members when they first join the NAI, at least annually thereafter, and in response to consumer complaints.[39] CDT believes that combining elements of both of these approaches will produce the most effective enforcement process.

CDT's preference would be to have an independent third party – unaffiliated with the NAI or any of its members – conduct compliance reviews. These reviews should be conducted when prospective members apply for NAI membership, annually, in response to consumer complaints, and potentially also at random. Having an independent third-party auditor will lend credibility to the results of the reviews, and ensure that all members receive fair treatment in the review process.

In addition, the documentation of compliance should be made public. The original NAI principles called for a summary report of member audits to be made publicly available on the NAI Web site. The NAI Principles 2008 indicate that both the annual summary relating to consumer complaints received and resulting enforcement actions and the policies and procedures for compliance reviews will be "made available upon request."[40] We see no reason why the NAI's transparency policy changed between 2000 and now, or why consumers, consumer advocates, and the press should have to specifically request compliance documentation. Both of these documents and the audit results should be made public on the NAI Web site.

Conclusion

CDT is pleased to be able to provide input into the NAI principles updating process. We are hopeful that the NAI and its members will carefully consider all comments that they receive in an effort to create the guidelines that best address the privacy issues involved in behavioral advertising.

The Internet and online advertising have changed dramatically in the eight years since the NAI was created, and they are bound to continue to evolve at a rapid pace. For this

[38] NAI Principles at 12.

[39] NAI Principles 2008 at 10.

[40] NAI Principles 2008 at 10.

reason, we believe the NAI should make updating the principles a regular occurrence, perhaps on a two-year interval. This will ensure that the internal pressures at the NAI that contributed to the last eight years of inertia on the principles will not continue in the future.

Some of the changes that we have suggested in our comments are major, but without them we believe the NAI will continue to be an inadequate framework for protecting consumer privacy online. In the absence of a general privacy law to safeguard consumer information, privacy-focused self-regulatory programs must be held to higher standards. We urge the NAI to answer that call and augment its principles to the benefit of the millions of consumers who view and interact with online advertising every day.

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