THE NETWORK ADVERTISING INITIATIVE: Failing at Consumer Protection and at Self-Regulation

Fall 2007

Pam Dixon
World Privacy Forum
November 2, 2007

Brief Summary of Report

This report examines behavioral advertising in the online and digital arena and specifically analyzes the effectiveness of the July 2000 industry and FTC agreement on self-regulation for behavioral ad targeting and delivery. The report finds that the agreement and the related self-regulatory body – called the Network Advertising Initiative or NAI – have failed to protect consumers and have failed to self-regulate the behavioral targeting industry.

The report reviews four areas of failure: 1) the NAI opt-out cookie does not work consistently and does not fulfill its purpose as a consumer protection mechanism; 2) the NAI static approach to self-regulation ignores new business models and emerging consumer tracking and profiling technologies and practices; 3) the NAI self-regulation does not include a majority of industry groups in the behavioral advertising sector; and 4) NAI's self-regulatory third party enforcement program lacks transparency and independence. The only success of the NAI has been lulling regulators into thinking that self-regulation fairly and effectively addresses the interests of consumers who are the targets of behavioral advertising.

Background of the Report

The Federal Trade Commission held a two-day workshop November 1-2, 2007 to revisit the issue of digital behavioral advertising. The World Privacy Forum testified at the workshop about the effectiveness of self-regulation and about other matters related to the NAI self-regulatory scheme. This report is part of formal written testimony to the Federal Trade Commission from the World Privacy Forum.

About the World Privacy Forum

The World Privacy Forum is a non-profit, non-partisan public interest research and consumer education group. It focuses on a range of privacy matters, including financial, health care, employment, and Internet privacy. The World Privacy Forum was founded in 2003.

Table of Contents

Table of Figures

Part I: Summary

When people sit at their computers and browse for new car information or to learn about the latest treatment for diabetes, when people walk down the street reading stock quotes on their mobile phones, and when people text a response for more information based on a television commercial they saw, their actions speak louder than words. A new realm of consumer tracking has grown up to translate these activities into advertisements. This kind of advertising is *behaviorally targeted advertising*. Behaviorally targeted advertising is as controversial as it is lucrative.

Behavioral advertising is *lucrative* because advertising based on a person's past actions has the potential to result in increased click-throughs and purchases. Behavioral advertising is *controversial* because in order to conduct behavioral-based advertising, advertisers may collect an extraordinary amount of personal information to figure out what makes a person tick. This information can range from demographic information like gender, race, ethnicity, and age to what kinds of web sites a person visited within the last month, how long they stayed on which pages, and what news articles they read. Often, this kind of tracking is completely invisible to consumers.[1]

Behavioral advertising was the subject of a Federal Trade Commission (FTC) workshop in 1999. It was the first time the FTC looked at the online aspects of behavioral advertising and consumer targeting. Subsequent to the workshop, the FTC worked with behavioral and other advertisers to craft a self-regulatory agreement that had as its goal to protect consumers from the negative aspects of behavioral advertising while still allowing companies to profit from the then-new Internet. That agreement was called the Network Advertising Initiative, or NAI.[2]

Does the NAI Self –Regulatory Agreement Work?

This report looks at the self-regulatory NAI agreement and the associated NAI industry organization and asks the question: does the NAI self-regulatory agreement and the related organization effectively achieve their stated goals of consumer protection in the behavioral advertising space? While few consumers have heard of the NAI and its

[1] For more information about the process of network advertising and consumer profiling, see *FTC Online Profiling: A Report to Congress,* June 2000.
<http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf >.

[2] The NAI is a self-regulatory plan for the network advertising industry crafted by industry in conjunction with the FTC and recommended by the Federal Trade Commission. See
<http://www.networkadvertising.org>. See also the discussion of the NAI in Part I of this report.

relationship to behavioral advertising,[3] the NAI nevertheless remains highly-promoted by the industry.

This report analyses the NAI implementation over the seven years of its existence and finds that the NAI has failed to meet the basic goals for which it was created.

The report focuses on four specific aspects of the NAI self-regulatory program:

1) The NAI opt-out cookie;

2) consumer tracking and profiling technologies and techniques and how they relate to the NAI self-regulation, including emerging tracking techniques such as Flash cookies, MS UserData, browser cache cookies, and other tracking technologies;

3) the membership of the NAI self-regulatory program; and

4) the NAI self-regulatory third party enforcement program.

Difficulties with the NAI

The failure of the NAI is significant from both a technical and a policy perspective. Most consumers who browse online using computers, mobile phones and other technologies are exposed to behavioral targeting, tracking, and advertising whether they are aware of it or not. The NAI opt-out cookie – arguably the centerpiece of the NAI self-regulation in terms of consumer protection from tracking – has failed. Consumers do not widely know about or understand the opt-out, the opt-out does not work reliably, and the opt-out does not persist reliably.

The static nature of the July 2000 NAI agreement is a major deficiency. Although technologies and techniques in the behavioral advertising sector underwent rapid maturation, the NAI agreement remained unchanged. The NAI has made no attempt to extend its self-regulatory structure to reflect developments in the Internet sector or in business practices. Its conception of online profiling grew rapidly stale. For example, techniques exist today for tracking of consumers that do not rely on traditional cookies. As time passed, the NAI self-regulation's effectiveness toward consumer protection became less effective or and less relevant.

Hidden tracking of consumers is something that the NAI was expressly supposed to prevent.[4] However, consumers affected by the new technologies do not typically have the

[3] Definition of behavioral advertising: *Advertising served to a consumer based on **behavioral tracking,** that is, the practice of collecting and compiling a record of individual consumers' activities, interests, preferences, and/or communications over time.* See *Consumer Rights and Protections in the Behavioral Advertising Sector*.
<http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf>.

right to choose whether their activities can be tracked by advertising companies. As a result, consumers have even less knowledge about or control over the detailed profiles about them, their lives, and their online and other digital activities and behaviors that result from the tracking.

Another promise of NAI self-regulation – that self-regulation would capture 90 percent of the industry – has not been accomplished. The membership record of the NAI is perhaps a model example of a failed self-regulatory effort. The independent, third party enforcement of the NAI self-regulatory body is of questionable independence, and has exhibited a troubling laxity and lack of transparency. These factors have contributed to an environment that values unfettered data collection more and implements consumers' rights of informational self-determination and privacy less.

The reason for self-regulation was to protect consumers from the negative aspects of unregulated profiling. The Federal Trade Commission acknowledged public comments and concerns recognizing that consumers who are the subjects of behavioral profiling and targeting may experience price discrimination and may ultimately be exposed to fewer or different economic, social, employment, and other opportunities based on behavioral information that may not be accurate, complete, fair, or even about them.[5] The information collected may be used for purposes far removed from advertising, and secondary uses of the information could harm consumers in other spheres. The NAI was put in place to prevent such harms from occurring, but it has failed to achieve its consumer protection goals.

Part II: Discussion

The Beginnings of the NAI

In 1999, when online advertising was still a fresh segment of the advertising sector, widespread concerns arose about the ways that consumers could be tracked and targeted online for advertising purposes. The Federal Trade Commission held a workshop on online profiling in November 1999.[6] The concerns of the day were distilled in a FTC report to Congress in June 2000, *Online Profiling: A Report to Congress*. In that report, the FTC found that online profiling presented privacy problems for consumers. The FTC found that online profiling was primarily accomplished through banner ads, cookies, and

---

[4] FTC *Online Profiling: A Report to Congress, Part 2, Recommendations* at pages 3-4. < http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>

[5] *Online Profiling: A Report to Congress*, page 13. <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>.

[6] A transcript of the Workshop is available at <http://www.ftc.gov/bcp/profiling/index.htm>.

web bugs, also called web beacons.[7] The Commission also concluded that online profiling was largely invisible to consumers:

> Although network advertisers and their profiling activities are nearly ubiquitous, they are most often invisible to consumers. All that consumers see are the Web sites they visit; banner ads appear as a seamless, integral part of the Web page on which they appear and cookies are placed without any notice to consumers. Unless the Web sites visited by consumers provide notice of the ad network's presence and data collection, consumers may be totally unaware that their activities online are being monitored.[8]

Self-Regulatory Effort Begun in 1999

In the spring of 1999, prior to its November workshop, the FTC invited network advertising companies to "discuss business practices and the possibility of self-regulation."[9] The companies announced the formation of the NAI at the 1999 November workshop.

These self-regulatory efforts were discussed in the first FTC report to Congress, which was published in June 2000.[10] No completed self-regulatory document was available for review at that time.

The FTC Recommends the NAI ….Paired with a Recommendation for Backstop Legislation

The Senate Commerce Committee held hearings on online profiling in June 2000. At that time, the Committee heard that privacy and consumer rights groups had not been involved in the NAI discussions with the consequence that a week later, seven senators on the Committee wrote urging the FTC to include privacy and consumer groups in the NAI talks. Some groups were invited to examine a mock up of the final NAI agreement on July 19.[11] On July 27, the final NAI agreement was released publicly in its final form in the FTC's second report to Congress on online profiling (July, 2000). In this report, the

---

[7] *Online Profiling: A Report to Congress*, pages 2-3. "In general, these network advertising companies do not merely supply banner ads; they also gather data about the consumers who view their ads. This is accomplished primarily by the use of "cookies"11 and "Web bugs" which track the individual's actions on the Web." < http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>.

[8] *Id*. at 6.

[9] *Id*. at 22.

[10] *Id*. at 22.

[11] For more about the lead-up to the final publication of the NAI agreement, see *Network Advertising Initiative: Principles not Privacy*, July 2000, EPIC and Junkbusters. <http://www.epic.org> and <http://www.junkbusters.com>. "Privacy and consumer groups were not allowed to retain or distribute any of the documents discussed."

FTC recommended the NAI as a self-regulatory solution to the problem of online profiling of consumers.

> The Commission commends the NAI companies for the innovative aspects of their proposal and for their willingness to adopt and follow these self-regulatory principles. Their principles address the privacy concerns consumers have about online profiling and are consistent with fair information practices. As the Commission has previously recognized, self-regulation is an important and powerful mechanism for protecting consumers, and the NAI principles present a solid self-regulatory scheme. Moreover, NAI members have agreed to begin to put their principles into effect immediately while Congress considers the Commission's recommendations concerning online profiling.[12]

The FTC also noted in its second report that legislation was needed to bolster the NAI:

> Nonetheless, backstop legislation addressing online profiling is still required to fully ensure that consumers' privacy is protected online. For while NAI's current membership constitutes over 90% of the network advertising industry in terms of revenue and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program. In addition, there are unavoidable gaps in the network advertising companies' ability to require host Web sites to post notices about profiling, namely Web sites that do not directly contract with the network advertisers; only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them.[13]

The NAI was drafted with the "full review and support of the FTC."[14] The FTC stated that the NAI self-regulatory principles were based on Fair Information Practices, including the canon of Fair Information Principles as articulated in 1980 by the Organization for Economic Cooperation and Development (OECD) and ratified by the United States.[15] Whether the NAI principles actually implement all Fair Information Practices is open to debate.

The FTC did not solicit formal or informal public comments on the NAI or on the FTC's blessing of NAI. The NAI was never debated publicly in any robust or formal manner. Nine network advertising companies signed the NAI founding document.[16]

---

[12] Federal Trade Commission. *Online Profiling: A Report to Congress Part 2 Recommendations*, July 2000. < http://www.ftc.gov/os/2000/07/onlineprofiling.pdf> at 9.
[13] *Id* at 10.
[14] <Networkadvertising.org/managing/principles.asp>, the NAI Principles: how they protect your privacy.
[15] *Online Profiling: A Report to Congress*, at note 4.
[16] The original NAI members were 24/7 media, AdForce, AdKnowledge, Avenue A, Burst Media, Doubleclick, Engage, L90, and Matchlogic. See *Network Advertising Initiative, Self-regulatory Principles for Online Preference Marketing by Network Advertisers*, July 10, 2000.

After the issuance of the FTC online profiling reports in 2000 and the FTC recommendation of the NAI self-regulation, industry perceived that the pressure for reform had diminished. The recommended legislation to prevent the self-regulation plan from failing for these reasons never happened. By 2002, just two years after the FTC recommended the NAI self-regulatory program, the NAI had only two member companies.[17] Once the external pressure diminished, the NAI began to fail. The FTC was correct when it stated in its report that "Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program."[18] Those were only some of the reasons for the NAI's failures, but they are significant ones.

What the NAI Does

The essential activity of the NAI is to define terms, discuss a handful of abbreviated consumer rights, which the NAI calls its "principles," and to set up a structure of "opt-out cookies."

The principles of the NAI are as follows:

> I. Network Advertising Initiative ("NAI") Overview
>
> A. Network advertisers will adhere to the Online Privacy Alliance ("OPA") Privacy Policies Guidelines for personally identifiable information.
>
> B. Network advertisers will not use sensitive personally identifiable data for online preference marketing.
>
> C. Network advertisers will not, without prior affirmative consent ("opt-in"), merge personally identifiable information with information previously collected as non-personally identifiable information.
>
> D. Network advertisers will provide consumers with robust notice and choice regarding the merger of personally identifiable information with non-personally identifiable information collected on a going forward basis for online preference marketing.
>
> E. Network advertisers will not use personally identifiable information ("PII") consisting of PII collected offline merged with PII collected online for online preference marketing unless the consumer has been afforded

[17] See Figures 5-8 in this document. See also <http://web.archive.org/web/20021206034703/networkadvertising.org/aboutnai_members.asp/>.
[18] *Online Profiling: A Report to Congress* at 10.

robust notice and choice about such merger before it occurs.

F. Network advertisers will require Web publishers with which they have contractual relationships to provide notice and choice regarding the collection of non-personally identifiable information for online preference marketing.

The principles are discussed in more detail in the body of NAI's 21-page agreement.[19]

The Underlying Concept of *Online* in the NAI Agreement and its Impact

NAI's basic approach to what *online* means is foundational to the functioning of the agreement.

- First, the NAI generally conceives of *online* as a **computer** connected to the **web**.

- Second, protections for consumers are built on this definition. As a result the NAI opt-out cookie (the core of the consumer protections) is conceived of as being delivered via the **web** to a **computer** accessing the web.

For example, in the FTC's report to Congress, the Commission defined online advertising largely as "banner ads displayed on Web pages – small graphic advertisements that appear in boxes above or to the side of the primary site content. Currently, tens of billions of banner ads are delivered to consumers each month as they surf the World Wide Web."[20]

The FTC's description of how online behavioral marketing worked was tied closely to the NAI's conception of online. The FTC wrote:

> An Illustration of How Network Profiling Works
> Online consumer Joe Smith goes to a Web site that sells sporting goods. He clicks on the page for golf bags. While there, he sees a banner ad, which he ignores as it does not interest him. The ad was placed by USAad Network. He then goes to a travel site and enters a search on "Hawaii." USAad Network also serves ads on this site, and Joe sees an ad for rental cars there. Joe then visits an online bookstore and browses through books about the world's best golf courses. USAad Network serves ads there, as well. A week later, Joe visits his favorite online news site, and notices an ad for golf vacation packages in Hawaii. Delighted, he clicks on the ad, which was served by the USAad Network. Later, Joe begins to

[19] *Network Advertising Initiative Self-Regulatory Principles for Online Preference Marketing by Network Advertisers*, July 2000. See p. 1, Overview.
[20] FTC Online Profiling Pt. 1 at 2.

> wonder whether it was a coincidence that this particular ad appeared and, if not, how it happened.[21]

The profile describes more activities, and discusses cookies:

> If an USAad cookie is not already present on Joe's computer, USAad will place a cookie with a unique identifier on Joe's hard drive.[22]

Note the emphasis on the use of computers and cookies.

From Kindergarten to Grad School: Maturation of the Behavioral Advertising Sector

The original description of profiling was fine for 2000, but it is out-of-date for 2007. The older profiling scenario still occurs, but profiling has matured significantly beyond this scenario. Even members of the advertising industry recognize this. TruEffect, an ad serving company, wrote in October, 2007, comments filed with the FTC that:

> The NAI "opt out" provisions were an essential step to ensure that ad servers offer consumers the option to participate or decline participation in online advertising tracking. Yet it's been eight years since the NAI principles were developed, and as the ad serving industry continues to evolve and change, they likely need to be revisited.[23]

The NAI opt-out cookie is squarely based on this kind of conceptualization of *online*. The NAI essentially limits itself to protecting consumers who are surfing the web from a computer and who download web-based NAI opt-out cookies – that was the model at the time. So under the 2000 NAI model, consumers who did not want their online computer activities tracked or their offline data merged with online data could download the NAI opt-out cookie. The opt-out cookie functioned to stop cookie-based profiling.[24]

So, for example, if a consumer with an NAI opt-out cookie browsed a shopping web site and bought something, a third-party network advertiser that tracked activities on the web site would not use the information to profile that consumer over time. When the consumer visited other web sites where the network advertiser employed tracking technologies, such as web beacons or pixel gifs or more cookies, the network advertiser would still not track that consumer because of the NAI opt-out cookie.

---

[21] *Id* at 6.

[22] *Id* at 7.

[23] Public comments of TruEffect, *FTC Town Hall eHavioral Advertising Tracking, Targeting & Technolgy November 1-2, 2007*, comments submitted October 19, 2007.

[24] See, for example, the FTC's *Online Profiling: A Report to Congress* (June 2000) for a description of how online profiling worked at the time on pages 6-7.

The New Scenario

In 2007, the online opt-out may still function, but an opt-out limited to classic web activity on a personal computer is myopic. *Online* today can mean a mobile phone or a Blackberry retrieving video, music, books, streams of text messages, or other forms of information. Video formats of ads allow for different kinds of tracking that go beyond what the NAI contemplated. Simply put, *online* today is much broader than an individual sitting at a computer connected to the Internet. Internet advertiser TruEffect acknowledges this in their comments to the FTC:

> The Internet is no longer defined by servers and browsers exchanging information across copper and fiber. **Going forward, data about consumer behavior will not be mediated by the cookie facility embedded in browser software, the management of which we have addressed to a degree through the NAI principles.** With the explosive growth of digitally addressable media including digital cable, satellite TV, and mobile, our customers are looking to us to provide technology solutions that will extend census-based measurement and dynamic targeting technology to these other channels.[25] [Emphasis added.]

The NAI agreement essentially limits itself to protecting consumers who are surfing the **web** from a **computer** and who download **web-based opt-out cookies**.[26] These foundational ideas undermine the effectiveness of the NAI in today's sophisticated ad sector. The NAI agreement, even if it functioned as designed, is simply not as useful today as a consumer protection instrument because the NAI has not been updated while the world has changed around it.

If the NAI self-regulation no longer adequately protects consumers, then that self-regulation has failed in its purpose. It is unlikely that any self-regulation scheme can successfully do the job it was intended to do when its foundation was built on rapidly aging models and when the self-regulatory organization has not updated that foundation.

The NAI is Broken and Does Not Protect Consumers

Although it is possible to identify many aspects of the NAI that are broken, this report focuses on four areas in particular: 1) the effectiveness of the NAI opt-out cookie as the primary tool for stopping tracking; 2) the applicability of the NAI to types of tracking that extend beyond the traditional cookie and to business models not expressly covered by the NAI; 3) the constantly shifting membership of the NAI; and 4) auditing and enforcement of the NAI.

---

[25] TruEffect public comments at 5.

[26] *Id*.

NAI "Opt-out Cookie" is a Failure

NAI opt-out cookies are a failure from a policy perspective and from a technical perspective.

Consumer Confusion

From a policy perspective, the concept of an opt-out cookie was too convoluted for consumers to understand from the beginning. It is counter-intuitive for consumers to go to a page to download a cookie onto their computer so that cookie will tell companies not to track them. Downloading one cookie so other cookies don't track you is a message most consumers never really heard or understood. Studies indicate that consumer confusion already exists regarding standard uses of cookies.[27]

Further, a new study finds that consumers, when they see the words "privacy policy," expect that their information will not be shared.[28] This suggests that many consumers will have difficulty fully understanding cookie functions in a meaningful way. It is reasonable to conclude that the opt-out cookie is just one more confusing aspect of cookies for consumers, and that consumers are not clear on what the opt-out cookie does or does not do in regards to privacy protections.

Consumers have other barriers regarding cookies: the shifting membership of the NAI has created an environment where a consumer has to be exceptionally vigilant to know if they have every downloaded every available opt-out cookie. When a member drops out of the NAI, a consumer has no way to know if a previously set opt-out cookie for that member still functions. Asking or expecting consumers to monitor the NAI website for this information is unreasonable.

Cookies by the Numbers

---

[27] A number of studies point to continuing consumer confusion about cookies. In particular, in a July 2007 study, InsightExpress found that "individuals who choose to delete cookies for one or more reasons possibly misunderstand the roles and functions served by cookie technology." The 2007 study found that 63 percent of respondents believed they had deleted their cookies, when only 23 percent actually had. The study was a repeat of a 2005 InsightExress study that found that of 59 percent of respondents who tried to delete cookies, only 35% of the "deleter group" studied were able to successfully delete their cookies. See *InsightExpress Study Sheds New Light on Cookie Deletion*, Business Wire, July 17 2007. See also *New Research Reveals Significant Consumer Misunderstanding of Cookies; Few Understand the Function of Cookies and Only 35% of Online Consumers are Able to Successfully Delete Them.* Business Wire, April 21 2005. These numbers are in line with comScore's examination of approximately 400,000 U.S. users in December 2006 which found that about 31 percent of U.S. computer users clear their first-party cookies in a month, with similar numbers for clearing third party ad network cookies. See *The Impact of Cookie Deletion on the Accuracy of Site-Server and Ad-Server Metrics: An Empirical comScore Study*, comScore, June 2007. <http://www.comscore.com>.

[28] See Research Report: *Consumers Fundamentally Misunderstand the Online Advertising Marketplace*, Joseph Turow, Deirdre K. Mulligan, Chris Jay Hoofnagle. University of Pennsylvania Annenberg School for Communication and UC-Berkeley Law's Samuelson Law, Technology & Public Policy Clinic.

Some of the questions that need to be asked about opt-out cookies are: how many consumers have downloaded opt-out cookies? How long do most consumers keep opt-out cookies? How do network advertisers pro-actively make consumers aware of their opt-out cookies? The answers to these questions are known by the network advertisers, who generally keep excellent track of their cookies.

One of the key issues that needs to be assessed is how many consumers actually know about opt-out cookies. One way to get at this is to determine how many consumers *use* opt-out cookies. If NAI members have detailed information about consumer use of opt-out cookies, that information has been shared with the public. The information would inform the debate, but it is also possible that the information would show further holes in the NAI self-regulatory scheme.

Some numbers do exist. TRUSTe, the current enforcer of the NAI agreement, used to report on NAI complaints about opt-out cookies. In March 2002, TRUSTe's first report on NAI enforcement documented that there were 30 complaints about the NAI, and every one of the complaints was about opt-out cookies. Complaints about opt-out cookies continued all the way through December 2004, the last month that TRUSTe reported opt-out cookie complaints publicly. It is unknown how many consumers are still complaining about opt-out cookies, as there is no longer any public reporting on them from TRUSTe. But even the limited TRUSTe reports that are available are revealing.

The Network Advertising Initiative, in public comments filed with the FTC in October 2007, said that in 2001, the NAI web site was visited 30,000 during its first week of operation.[29] NAI also commented that: "…in 2006 we estimate that our opt-out page was visited 1,003,750 times." It is unknown if these were unique visitors, and it is unknown how many of those visitors opted-out successfully. It is also unknown what percentage of visitors to the opt-out site this constitutes compared to the universe of consumers who have had behaviorally-targeted network ads served to them.[30]

What policy makers need to know is how many consumers are opting out, and for those who are not opting out, why they are not opting out. Is it because the majority of consumers have never heard about an NAI opt-out? Or is it because consumers cannot opt-out easily? Or are there other reasons?

Technical problems have cropped up with the opt-out cookie -- NAI opt-outs are not simple to accomplish for everyone. Unfortunately, those consumers who manage to hear about an NAI opt-out and who go to the NAI opt-out page with browser cookies turned

---

[29] Public Comments of the Network Advertising Initiative, *Network Advertising (NAI) Written Comments for the FTC's Ehavioral Advertising Town Hall Forum*, October 19, 2007. <http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf>.

[30] The privacy policy on the NAI website says that NAI becomes the "sole owner of all information collected on this site." If a consumer who is confused about an opt-out cookie fills out an NAI "contact us" form, the privacy policy language suggests that NAI becomes the "sole owner" of the consumer's name, email address, and other information. It isn't clear whether the statement in the privacy policy has any real meaning or effect, but it is an example of where a self-regulatory body has not adequately thought through the consumer perspective of the process. <http://www.networkadvertising.org/about/privacy.asp>.

off encounter unfriendly error messages. These consumers may have increased barriers in finding detailed instructions on opting out. Consumers who have cookies turned on may still have problems opting out, something the NAI admits on its own pages.

Opt-out Web Pages do not Always Work

Those seeking to opt-out of tracking by NIA members must visit <www.networkadvertising.org> with cookies turned on. After landing on the home page, consumers who click the opt-out button on the page are sent to the NAI opt-out page. The page offers checkboxes that correlate to an opt-out for different NAI members. Each check box should result in the setting of a separate opt-out cookie on the consumer's computer. However, the results are highly variable, and the opt-outs often are not successfully set.

In a series of tests using different computers, IP addresses, browser types, and operating systems, the World Privacy Forum tested how well the official NAI opt-out page was working.[31]

The Forum also invited others to opt-out and report on their experiences. One individual who tried to opt-out sent in a pithy note: "It didn't work so well" accompanied by a screen shot of the results of his opt-out effort. The screen shot revealed that only two of the opt-outs on the page had actually worked for this consumer.[32]

World Privacy Forum tests demonstrated that opt-outs on the NAI page do not always work even when browsers are optimally set to accept all cookies. Even when different kinds of web browsers were set to accept all cookies, the opt-out cookies were not always set properly. It is difficult to offer a hard number for the failure rate for setting NAI opt-out cookies due to the high variability in the causes for failure. However, for some standard computer operating systems and browsers, the failure rate exceeds 50 percent, depending on the computer set-up, firewall settings, and many other factors.

For example, in one test run, using computers running Firefox or IE on MS Windows and Safari on Mac OSX, World Privacy Forum tests found that checking the multiple opt-out boxes offered by NAI resulted in only some NAI opt-out cookies being set successfully. (The NAI opt-out page has a feature that tells users whether the opt-out was successful or not.) Using a computer running Mozilla on a SUN Ultra, and a computer running Firefox on Mac OSX, one test found that the opt-out worked. However, firewall settings can influence these results, so there is high variability of opt-out success or non-success.

The NAI opt-out page – Having Trouble Opting Out? –
addresses these issues and says:

[31] The page the WPF tested was <http://www.networkadvertising.org/managing/opt_out.asp>.
[32] The email is on file at the WPF offices and is available, but is only available redacted of personally identifiable information about the consumer.

> The performance of the global opt-out tool might be affected by a number of factors outside the control of the NAI and/or its member ad networks. These factors include corporate network security, telecommunications breakdowns, browser settings, ISP or infrastructure anomalies and client-side technical glitches, among other possible issues.[33]

The NAI is well aware of the problems with the opt-outs. In its public comments to the FTC in October 2007, the NAI wrote:

> The single most common issue raised by consumers about the NAI Principles program relates to the functionality of the opt-out. It is rather common for consumers to request assistance to ensure that their opt-out cookie is functioning properly (browser compatibility concerns). The vast majority of these concerns are successfully addressed by having a staff member work directly with the consumer to resolve the problem they had been experiencing.[34]

It would be helpful to know how often consumers spoke to or communicated with NAI staff, and the specific results of those contacts.

Another problem with the NAI opt-out site is that if a computer is set not to accept cookies at all, the consumer who clicks on the NAI opt-outs will see an unfriendly error page. The NAI does not offer an explanation on the error page that in order for the opt-out to work, that cookies must be accepted. Because cookies are at the heart of the NAI self-regulatory model, helping consumers to understand cookies would seem to be a core element of any well-intentioned program.

Given the large variety of computer types, machine configurations, corporate and personal firewall configurations, web browsers and browser configurations, it would be appropriate for NAI to provide detailed assistance on its website that reflects the variety and complexities of Internet usage.

Even if NAI provided the information that consumers need to make use of opt-out cookies, problems with the NAI opt-out will remain. It is far from clear that any opt-out cookie should be the mechanism of first choice for consumer protection at all, given all of the difficulties.

The Opt-Out is Susceptible to Deletion

Opt-out cookies only work when they have been downloaded to a user's hard drive and stay there. Opt-out cookies may be deleted by users who delete all of their cookies at one time, no matter what kind of cookies they are. Consumers who run a security protection

---

[33] NetworkAdvertising.org < http://www.networkadvertising.org/managing/optout_problems.asp>.See also < http://www.networkadvertising.org/managing/faqs.asp#question_16>.

[34] Public Comments of the Network Advertising Initiative, FTC, October 19, 2007. <http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf>.

program that removes spyware and malware may erase NAI opt-out cookies. Some consumers operate these programs as a standard part of their computer hygiene routine.

Unless a consumer is highly knowledgeable about cookies and is able to distinguish opt-out cookies from other cookies, consumers may not be able to maintain their opt-out cookies over time. These problems with reliance on opt-out cookies are not new, and they have been known for many years.

There is no simple or universal solution for this problem of deleting the opt-out cookie. One solution that has been proposed is Tacoda's so-called "hardened opt-out." This approach uses a file stored in a user's browser cache to restore an opt-out cookie that was deleted. An undisclosed overriding of a consumer's choice may be a chilling precedent, and it is discussed in more detail below under the heading *Browser Cache Cookies*.

Can any self-regulation effort rely on a mechanism so fragile that every time a consumer runs a computer security program, the core aspect of consumer protection disappears from a consumer's computer? It doesn't make sense to base a self-regulatory scheme on something like the NAI opt-out cookie given its high failure rate.

Even if some of the difficulties can be attributed to developments with computers (e.g., the spread of anti-spyware and malware programs), it is curious that NAI made no apparent attempt to change or update its methodology. It is entirely possible that NAI members are happy to continue offering the consumer NAI opt-out program, despite the acknowledged problems with the NAI opt-out and despite low consumer adoption of the program.

Cookie Blocking Has Led to the Use of Other Persistent Identifiers and Tracking Mechanisms

Several studies have reliably shown that about 30 percent of consumers delete cookies.[35]

One response to this by the advertising industry has been the development of ways to identify or re-identify users who have blocked or deleted cookies. For example, a patent filed by David R. Morgan and others in 2005 – *Network for matching an audience with deliverable content* – addresses how to circumvent cookie blocking. The patent boasts that users can be re-associated with their profiles even if they have deleted cookies, and even if they are using different machines:

> Cookie blocking technologies have become an increasing problem for online publishers. […]
>
> That is, an audience member can be reconnected with their data after cookies may have been deleted – or even if the audience member moves to a different client machine.

[35] See *supra* note 27.

[…]

> In connection with a visit to any site within the network, an authoritative identification is received 2008. This information may be received in the absence of the NPRID. The authoritative identification identifies the profiled audience member in connection with activity, and is used 2010 to correlate the profiled audience member in the NPRID. In turn, the NPRID is associated to the cookie related information as described. This allows a comparison 2012 of the cookie information connected with the current activity with that stored in association with the NPRID. Such information can be used to update 2014 the cookie information in association with the audience member's browser, even if the cookies have been deleted between past profiling and the current browsing activity, or even if the audience member uses a different machine (if desired). Such updating may of course entail restoring the cookie information previously established for this particular audience member. [36]

Re-identification of users is not a surprising or even a new application of technology. The application goes beyond the limited NAI conception of cookies and tracking and illustrates how irrelevant it is becoming. Nevertheless, the expanded tracking capability that technology allows is something that the NAI has ignored. In the absence of constant external pressure, the NAI seemingly has no incentive to address new technology used to track consumers. The failure of NAI to change raises the question of NAI effectiveness as a self-regulatory organization.

Beyond Cookies: Tracking Technologies are not Always Exposed or Visible to Consumers

A traditional cookie as defined by the NAI is not the only persistent identifier and tracker available to network advertisers and marketers anymore. New technologies and techniques have become routine business practice since the original NAI was written, particularly in the area of persistent identifiers and tracking technologies. A rich array of browser cache cookies, Flash cookies, and other non-NAI-covered tracking techniques not only exist, but are in use today.

The problem with the non-NAI covered techniques and technologies is that consumers, even if they download an NAI opt-out cookie, may still be tracked in ways hidden to them. Further, opt-in or opt-out choices made by consumers are in some cases ignored and overridden by industry uses of non-NAI covered tracking techniques. The NAI does not apply to these tracking techniques. The result is that the NAI is apparently not even trying to self-regulate all the tracking activities that should fall under its purview.

[36] United States Patent Application 0050166233, Sections -0199-0200, 0212.

Secret Browser "Cache Cookies," or, Non-Consensual Cache-Tracking

Browser "cache cookies" refer to a way of tracking users that was not addressed in the NAI agreement. The NAI use of the word *cookie* refers to a precise cookie standard generally recognized as defined by the IETF standards.[37] The NAI opt-out cookie does not address anything other than an IETF-style of cookie. **Therefore, companies that use and store persistent identifiers not covered by the narrow NAI cookie definition can, on a technical level, both comply with the NAI and still persistently track users.**

One potent example of this is the browser cache cookie, sometimes called the **secret cache cookie**.[38] Browser cache cookies are not a new idea. In fact, they were written about and discussed prior to the original NAI agreement.[39] A browser cache cookie loads a persistent identifier into the browser cache area of a consumer's computer. Very few, if any, consumers know to clear out their browser cache to remove persistent identifiers. That is one allure of this type of tracking technique to those doing the tracking.

Several patents and or patent applications exist in the area of browser cache cookies, and there are a number of known variations of browser cache-based tracking techniques. One patent application discusses browser cache cookies as "secret cache cookies."[40]

One technologist noted that "**it seems irrational for browsers to provide selective control over treatment of cookies, without providing similar control over other mechanisms that are equally effective for storing and retrieving state on the client**."[41] The same broad observation may be applied to the NAI agreement. Why does the NAI agreement provide for self-regulation of the industry's use of traditional cookies, while staying silent on known alternative tracking techniques such as browser cache cookies?

Tacoda's "Hardened Opt-Out" Overrides Consumers' Deletion Choices and is not Consensual

A current member of the NAI, Tacoda is a network advertiser that conducts behavioral ad targeting. Its CEO stated that the Tacoda network includes approximately 4000 web sites and reaches about 125 million "uniques" per month.[42] Current Tacoda press releases also state that it is developing patent-pending technology "to recognize a consumers' opt-out

---

[37] Internet Engineering Task Force, *HTTP State Management Mechanism*, February 1997. <http://www.ietf.org/rfc/rfc2109.txt>.

[38] Technical note: In this report, a browser cache cookie means the eTag and similar techniques.

[39] Martin Pool, *Meantime: Non-consensual http user tracking using caches*, March 2000. <http://sourcefrog.net/projects/meantime/ >.

[40] Jakobsson; Bjorn Markus; et al, US Patent Application 20070106748. May 10, 2007 at 16, 17, 19.

[41] See Collin Jackson, et.al, *Protecting Browser State from Web Privacy Attacks*, WWW 2006, May 23.26, 2006, Edinburgh, Scotland.ACM 1-59593-323-9/06/0005 (emphasis added).

[42] Remarks of Curt Viebranz, CEO of Tacoda. BM 2007, *Grilling the Vendors*, Panel Discussion. July 24 2007. Video: < http://www.brightcove.tv/title.jsp?title=1125952443&channel=429048905>.

status even if they have deleted their browser cookies. Current opt-out systems are not able to do this."[43] In July, 2007, executives from Tacoda referred to something they call a "hardened opt-out" during panel discussions at the MediaPost Behavioral Marketing Forum. Larry Allen, SVP Marketing, Tacoda noted that:

> One of the other interesting things about privacy is if you do opt out of many networks, and then you accidentally clear your cookies, you've just re-opted in to all of the ad networks you opted out of, except Tacoda. So, one of the things that we did is we built some technology that enabled us to harden the opt-out and enable that we uphold your choice.[44]

Curt Viebranz, CEO of Tacoda, also discussed the hardened opt-out on another panel:

> One of the little known secrets is that the ability -- as with the Tacoda audience networks -- the ability to opt out is driven by a cookie itself. So that if you go to the Network Advertising Initiative -- of which we're part -- and you opt out, and subsequent to that you clear your cookies, de facto you're going to pick up a Tacoda cookie the next time you visit one of our sites. So we are actually trying ...(pause) We believe that ultimately we are going to have a trusted relationship with the consumer as a purveyor of topical information. It's going to get there at some point, and so we're basically saying is we're going to notice consumers that they're part of our network, if they choose to opt out, and we notice in the cache that they have actively opted out, we're going to reset that cookie to allow them out.[45]

This "hardened opt-out" works through one of the known variations of the browser cache cookie technique. Specifically, Tacoda uses an ENTITY TAG, or eTag that is stored in the cache of the user's web browser. This eTag interacts with the Tacoda servers and users' computers to identify users and some of their past actions. Based on the MediaPost statements, even if a user has deleted the Tacoda NAI opt-out cookie, Tacoda, employing the browser cache technique, effectively re-sets that cookie and acts as though the user had not deleted the Tacoda NAI opt-out cookie.

This is what part of the interaction looks like (Test done using Internet Explorer):

> Tacoda looks to see if this file is in the local browser cache:
>
> `http://an.tacoda.net/optout/ooverify.js`

---

[43] Market Wire, *Tacoda Launches Consumer Choice Initiative; Plans Opt-Out Preservation With New Patent-Pending Technology*. November 6, 2006.

[44] Remarks of Larry Allen, SVP Tacoda. BM 2007, *Is Privacy the Third Rail*? Panel Discussion. July 24 2007. Video: <http://www.brightcove.tv/title.jsp?title=1126051143&channel=429048905>.

[45] BM 2007, *Grilling the Vendors*, Panel Discussion. July 24 2007. Video: < http://www.brightcove.tv/title.jsp?title=1125952443&channel=429048905>.

If it isn't, then a unique ID number for the file is sent as an eTag:

```
ETag: "18b9b040b0c918904b0155e1c6ad3781:1172245630"
```

If the opt-out page is accessed again, this unique ID number is sent back in an "If-None-Match" header:

```
If-None-Match:
"18b9b040b0c918904b0155e1c6ad3781:1172245630"
```

The cache of a web browser is not where traditional NAI cookies are stored, and very few users would think to look in their browser's cache for a persistent identifier. As the items in the cache age, older items are removed and replaced with newer items in the cache. Few consumers are aware of the reasons to delete their browser cache along with their traditional cookies. Although cache control is not as popular as cookie control yet, Mozilla Firefox has an extension called Safecache (www.safecache.com) that, if used properly, can help alleviate cache tracking.[46]

On first blush Tacoda's attempt to "harden" or protect the NAI opt-out from user deletion may appear to be a good thing. But the reality is that resetting cookies without consumer consent is a bad precedent. Overriding an action taken by a consumer can be used for bad purposes or for good purposes. Resetting a deleted opt-out cookie may seem to be a neutral activity, but the spread of cookie resetting actions is more likely to be harmful to consumers. If this negative precedent becomes an established technique, not all companies using the technique can be trusted to reset cookies honorably. Assumptions about what the consumer actually meant are not likely to be made fairly or honestly by companies profiting from advertising.

Given that browser cache activities are not covered under the NAI, consumers have no NAI protections in this area. This is another example where the NAI has failed to address new techniques not covered in the NAI agreement.

Flash Cookies

Flash cookies are typically deposited when a user plays a video on the web. Watching most YouTube videos, for example, will often set a Google Flash cookie. While it was never intended as a persistent tracking device, the Adobe Flash[47] program's Local Shared Objects (LSO) function allows the storage of persistent unique identifiers from third parties.[48]

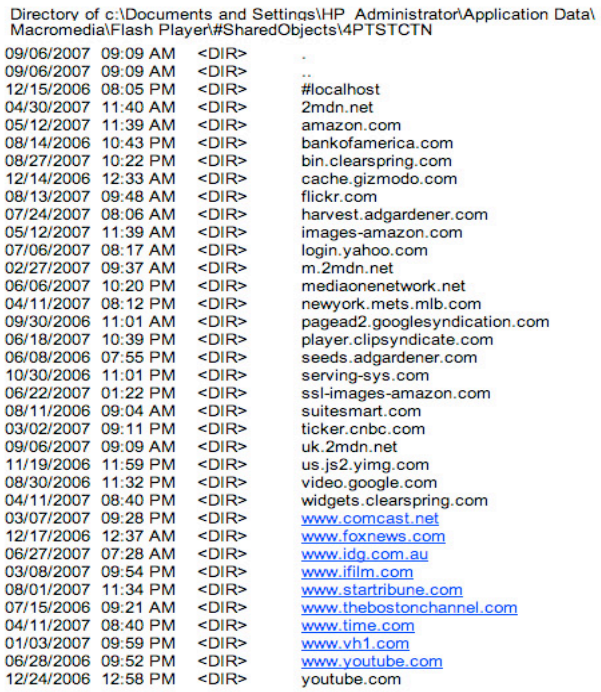
---

[46] The use of browser caches to set and track persistent identifiers as well as Mozilla Safe Cache is discussed in detail in Collin Jackson, et.al, *Protecting Browser State from Web Privacy Attacks*, WWW 2006, May 23.26, 2006, Edinburgh, Scotland.ACM 1-59593-323-9/06/0005.

[47] >http://www.adobe.com/products/flash/>.

[48] There is also the capacity of Remote Shared Objects, which appear to be rarely used. RSOs function similarly to LSOs. See note 34.

Nicknamed "Flash cookies," or "third party Flash cookies," these tracking files reside in a folder outside of the traditional NAI-defined cookies folder. Flash cookies function similarly to cookies in terms of their tracking capabilities. (See Figure 1.) The functionality has not been lost on those seeking to track consumers and avoid the NAI restrictions.



Directory of c:\Documents and Settings\HP_Administrator\Application Data\Macromedia\Flash Player\#SharedObjects\4PTSTCTN

09/06/2007	09:09 AM	<DIR>	.
09/06/2007	09:09 AM	<DIR>	..
12/15/2006	08:05 PM	<DIR>	#localhost
04/30/2007	11:40 AM	<DIR>	2mdn.net
05/12/2007	11:39 AM	<DIR>	amazon.com
08/14/2006	10:43 PM	<DIR>	bankofamerica.com
08/27/2007	10:22 PM	<DIR>	bin.clearspring.com
12/14/2006	12:33 AM	<DIR>	cache.gizmodo.com
08/13/2007	09:48 AM	<DIR>	flickr.com
07/24/2007	08:06 AM	<DIR>	harvest.adgardener.com
05/12/2007	11:39 AM	<DIR>	images-amazon.com
07/06/2007	08:17 AM	<DIR>	login.yahoo.com
02/27/2007	09:37 AM	<DIR>	m.2mdn.net
06/06/2007	10:20 PM	<DIR>	mediaonenetwork.net
04/11/2007	08:12 PM	<DIR>	newyork.mets.mlb.com
09/30/2006	11:01 AM	<DIR>	pagead2.googlesyndication.com
06/18/2007	10:39 PM	<DIR>	player.clipsyndicate.com
06/08/2006	07:55 PM	<DIR>	seeds.adgardener.com
10/30/2006	11:01 PM	<DIR>	serving-sys.com
06/22/2007	01:22 PM	<DIR>	ssl-images-amazon.com
08/11/2006	09:04 AM	<DIR>	suitesmart.com
03/02/2007	09:11 PM	<DIR>	ticker.cnbc.com
09/06/2007	09:09 AM	<DIR>	uk.2mdn.net
11/19/2006	11:59 PM	<DIR>	us.js2.yimg.com
08/30/2006	11:32 PM	<DIR>	video.google.com
04/11/2007	08:40 PM	<DIR>	widgets.clearspring.com
03/07/2007	09:28 PM	<DIR>	www.comcast.net
12/17/2006	12:37 AM	<DIR>	www.foxnews.com
06/27/2007	07:28 AM	<DIR>	www.idg.com.au
03/08/2007	09:54 PM	<DIR>	www.ifilm.com
08/01/2007	11:34 PM	<DIR>	www.startribune.com
07/15/2006	09:21 AM	<DIR>	www.thebostonchannel.com
04/11/2007	08:40 PM	<DIR>	www.time.com
01/03/2007	09:59 PM	<DIR>	www.vh1.com
06/28/2006	09:52 PM	<DIR>	www.youtube.com
12/24/2006	12:58 PM	<DIR>	youtube.com

Figure 1: A User's Collection of Flash cookies accumulated from browsing the web.

Flash cookies are not identical to traditional cookies. They are stored in a different area than a traditional cookie, and Flash cookies have a much larger capacity for storage.[49] Although most companies use Flash cookies to simply store a numeric identifier that links back to a server (similar to a traditional cookie), it is possible for a company to store more information in the Flash cookie file.

Adobe Flash describes Flash cookies in this way:

> A local shared object, sometimes referred to as a "Flash cookie," is a data file that can be created on your computer by the sites that you visit. Shared objects are most often used to enhance your web-browsing experience, for example, by allowing you to personalize the look and feel of a website that you frequently visit. Shared objects, by themselves, can't do anything to or with the data on your

[49] Adobe Tech Note: What is a local shared object? <http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_16194&sliceId=1>.

computer. More important, shared objects can never access or remember your e-mail address or other personal information unless you willingly provide such information.[50]

Adobe itself notes that *third party* local shared objects have implications for privacy and for tracking that users need to be concerned about:

> A *third-party local shared object*, sometimes referred to as a "third-party Flash cookie," is a shared object created by third-party content, or content that is not actually located on the site you are currently viewing. Third-party local shared objects may be important for privacy discussions because they can be used to track your preferences or your website usage across different websites that you visit.[51]

Adobe has a web site that allows users to set the LSO folder in ways that can include rejecting flash cookies altogether.[52] (See Figure 2 for what this looks like). However, most users do not know about Flash cookies, and even fewer know how to manage or disable Flash cookies.

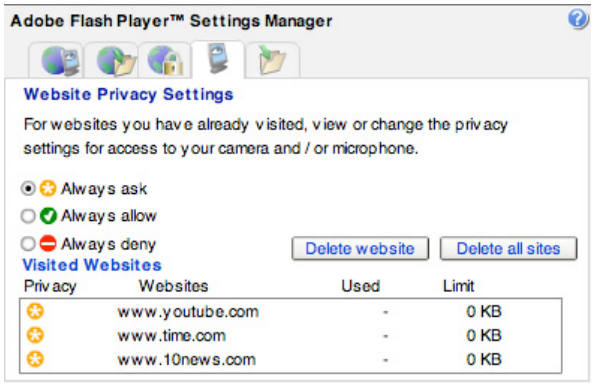


Figure 2: Adobe Flash Player Website privacy settings panel. The setting for this panel is set so that no information will be stored in the Flash cookie.

The NAI is silent about Flash cookies. The NAI agreement does not cover these increasingly popular forms of third-party tracking cookies. An NAI opt-out cookie, if

---

[50] Adobe. How to Manage and Disable Local Shared Objects. <http://kb.adobe.com/selfservice/viewContent.do?externalId=52697ee8&sliceId=1>. See the Flash cookies page at the Electronic Privacy Information Center web page, <http://www.epic.org/privacy/cookies/flash.html>.

[51] *Id.*

[52] The Adobe Flash preference manager is available at "How to manage and disable Local Shared Objects": <http://kb.adobe.com/selfservice/viewContent.do?externalId=52697ee8&sliceId=1>. There is a demo available that gives step-by-step advice on how to restrict Flash cookies.

downloaded, does not disable tracking that uses third party Flash cookies. Some have estimated that 98 percent of computers have Flash and therefore the ability to store Flash cookies.[53] As advertising transitions to being more video-based,[54] Flash cookies could become increasingly important for consumers to know about. Even if someone opted out of NAI tracking cookies, a company could deposit a third party Flash cookie or LSO with a tracking number. The effect could be the same or similar as third party tracking cookies. It is not known whether any NAI members use Flash cookies.

Flash cookies point up yet again the narrowness of the NAI agreement. These persistent – and effectively secret – identifiers that can track consumers are not included in NAI's self-regulation. It is further evidence of the failure of the NAI to accomplish its stated goal. Given the popularity of video and video ads, this deficiency is potentially substantial.

Silverlight Cookies

Microsoft Silverlight is a program that is a competitor to Adobe Flash. Silverlight cookies function similarly to Flash cookies. The Microsoft product is slightly different than the Flash product, however. Microsoft calls the Silverlight file an Isolated Storage File, and expressly describes it as a "hidden file" that can accept a unique identifier:

> The root of the virtual file system is located in a per-user, hidden folder in the physical file system. Each unique identifier provided by the host will map to a different consistent root, giving each application its own virtual file system. [55]

Microsoft does not provide users a way to simply or easily find or delete the hidden folder files at this time, nor does Microsoft address the issue of how Silverlight cookies may be used for depositing unique identifiers and tracking.

The NAI does not address the use of Microsoft's hidden file Silverlight cookies that include unique identifiers.

XML SuperCookie (Microsoft UserData)

---

[53] Matt Marshall, *New cookies, with PIE, are harder to throw out.* Sunday Gazette-Mail, Charleston, W.V. May 1, 2005.

[54] See, for example, Catherine Holahan, Business Week Online, *Online video ads: Just wait; A study by eMarketer predicts the floodgates will open after 2011.* See also *Web video ads to grow this year: Survey*, Prism Insight, March 19 2007. See also Wireless News, Oct. 30, 2007, reported that Bright.Spot TV had surpassed its one millionth video ad: "BrightSpot Media, creator of BrightSpot.TV, an emerging interactive video advertising network, announced that it will surpass one million video ads served, in the month of October."

[55] *See*: Microsoft Silverlight, *How To: Use Microsoft Isolated Storage with .NET Framework*, <http://silverlight.net/QuickStarts/IsoStore/StoreData.aspx>.

Yet another way an advertiser can potentially set a persistent tracking identifier is on a PC running Internet Explorer. This is a variation of a browser cache cookie. The storage depot in this case is in the Internet Explorer browser cache. (UserData is not available in any other browser except for IE). UserData is written to a hidden file and stored as an XML document. This data can be made to persist through reboots and a variety of other situations. These kinds of persistent identifiers have been called "super cookies" by some due to their large capacity.[56]

Like other non-NAI-covered persistent identifiers, MS UserData is not covered under the NAI agreement. MS UserData supercookies would be difficult for the average user to know about, find, or manage. When data is written in a hidden file, a typical user does not see it or ever know about it.

In its documentation of UserData, Microsoft included this security alert:

> Data in a UserData store is not encrypted and therefore not secure. Any application that has access to the drive where UserData is saved has access to the data. Therefore it is recommended that you do not persist sensitive data like credit card numbers. [57]

The warning continues:

> The UserData behavior persists information across sessions by writing to a UserData store. **This provides a data structure that is more dynamic and has a greater capacity than cookies.**[58] (Emphasis added.)

Figure 3, below, shows what UserData files look like when exposed. Most people would not know about these files nor know where to look for them.

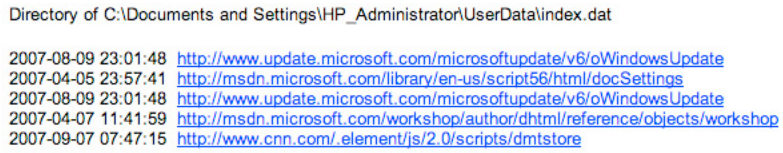


Figure 3: Screenshot of MS UserData files on a computer.

---

[56] *See:* Scott Isaacs, *Inside Technique: Building Site Favorites with XML Super-Cookie*, <http://www.siteexperts.com/tips/xml/ts05/page1.asp>. See also MSUserData. *Introduction to Persistence*, <http://msdn2.microsoft.com/en-us/library/ms533007.aspx> and <http://msdn2.microsoft.com/en-us/library/ms531424.aspx>.

[57] MSDN UserData Behavior <*http://msdn2.microsoft.com/en-us/library/ms531424.aspx*>.

[58] *Id.*

It is not known how widely MS UserData is being used today, but some companies do use it, as seen in Figure 3. A recent paper describes the idea of using browser states for tracking consumers and notes that a "same-origin principle" needs to be in effect in order to protect web browsers from this problem.[59] The same-origin principle would require that any entity that set a tracking mechanism to a web browser would be the only entity that could then access this information or read it. This is how traditional cookies work, but it is not how other tracking technologies employing browser states works. The NAI could have addressed this, but did not, and this reflects another point of failure of the self-regulation.

Persistent Identifiers in Other Devices

Consumers who access content using Mobile phones and other devices also need protection from persistent identifiers set on those devices. It is difficult to imagine that a person using a mobile phone would scroll through a lengthy privacy policy to find the option to click on an NAI opt-out cookie that would likely not work for the phone.

Mobile phone ads are already in place and are not a future technology. For example, a company named Decktrade is already delivering ads to the mobile web.[60] Ad network 24/7 debuted a mobile marketing ad network in April 2007.[61] MoPhap, a mobile advertising network that does behavioral targeting, announced a partnership in August 2007 that would allow them to conduct mobile third party ad serving.[62] Revenue Science announced in September of 2007 its plan to deliver behaviorally targeted ads to mobile phones in Japan that were able to browse the web.[63]

There is a great deal that is not known about consumer tracking on devices other than personal computers. For consumers, tracking on other devices is one more area where the NAI does not provide any protection. A good example of just how difficult this question is to address can be found in a recent Canadian Internet Policy and Public Interest Clinic study on Digital Rights Management and consumer privacy. The researchers for the study expressed surprise after encountering DoubleClick presence in a digital audio book from the library.[64]

---

[59] See Collin Jackson, *et al*, *Protecting Browser State from Web Privacy Attacks*, WWW 2006, May 23-26, 2006, Edinburgh, Scotland. ACM 1-59593-323-9/06/0005. <http://www2006.org/programme/files/xhtml/3536/index.html>.

[60] See Decktrade <http://www.decktrade.com/pages/advertisers?gclid=CNyV8Y3uso8CFR-YYAoduVhKLw>.

[61] Dianna Dilworth, *24/7 debuts mobile marketing ad network*, DMNews, April 6, 2007.

[62] Wireless News, *MoPhap Teams with RealTechNetwork*, August 19, 2007. "MoPhap is the only mobile ad serving company that has enabled third-party ad serving – the very same model that changed the face of online advertising."

[63] Reuters, *Revenue Science offers behavioral ads in Japan*, September 24, 2007.

[64] *Digital Rights Management and Consumer Privacy: An Assessment of DRM Applications under Canadian Privacy Law*, CIPPIC, September 2007. <http://www.cippic.ca>.

Much work needs to be done to expose all relevant technologies and to provide appropriate consumer rights and protection. This work should have been accomplished through a sincere self-regulatory process. However, as discussed, the NAI agreement only touches on narrow categories of technologies.

As a technology-specific instrument, the NAI agreement fails to address developing tracking techniques and mechanism, some of which were in use at the time the agreement was crafted. The NAI is not an effective self-regulation process because it does not expose all tracking technologies to consumers and because it allows for hidden and secret tracking. The NAI is the equivalent of a traffic safety organization that continues to offer consumers protections against horses and buggies long after the introduction of automobiles.

Membership Problems of the NAI

For a formal self-regulatory group, the NAI membership includes only a fraction of the industry engaging in behavioral ad targeting. The low numbers have plagued the NAI for its entire existence. One aspect of the problem has been the establishment of a non-full compliance membership category.

Low Numbers

When the FTC approved the NAI agreement, the understanding was that the self-regulatory body was going to include the majority of the industry players.

> The bedrock of any effective self-regulatory or legislative scheme is enforcement. In a self- regulatory context, this means that **nearly all industry members subject themselves to monitoring for compliance** by an independent third party and to sanctions for non-compliance, which may include public reporting of violations or referral to the FTC. [65] [Emphasis added.]

In November 2000, the year the FTC approved the NAI agreement, 12 companies were listed as members. However, just one year after the NAI was formed, the membership consisted of five members. In 2002 and 2003, only **two** companies remained as members of the NAI. (See Figure 4). Companies have dropped out of and rejoined the NAI at will over the years, without any apparent consequence. The NAI website does not maintain a list of past members or show the dates members joined and dropped out of NAI. The only way that past membership could be determined was by reviewing obsolete pages stored by Archive.org.

[65] Federal Trade Commission *Online Profiling Part2*, July 2000 at 8.

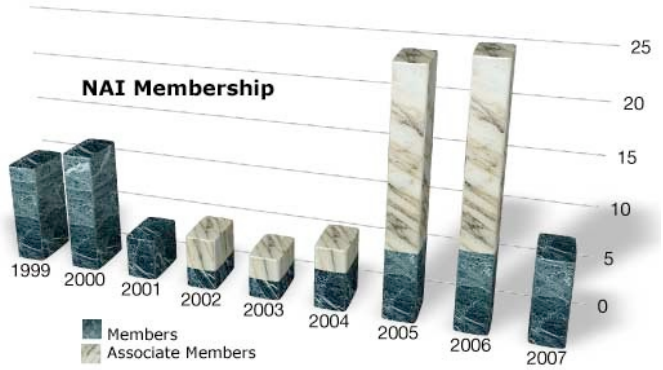


Figure 4: NAI Membership from 1999-2007. Note that only 2 members existed in 2002 and 2003. Associate Members of the NAI were not required to comply with the NAI principles.

The behavioral advertising industry itself is aware of the NAI membership issue. At the 2007 Behavioral Marketing Forum, ad industry expert Alan Chapell said in a panel:

> There are at least 50 companies that are holding themselves out to be behavioral targeting companies, and there are about 10 companies give or take who are full compliance members of the NAI. So when less than 20 to 25 percent of the industry is participating in the industry's own self-reg[ulatory] program, that's kind of a flare that's sent up to the FTC saying, well, what is the value of this program?
> …
> For me, I think the number one privacy issue is that the industry in and of itself has not embraced self-reg[ulation].[66]

It does not appear that, at any time since 2000, NAI has represented a majority of the industry.

NAI Allowance of Non-Full Compliance Associate Members

The NAI established a "non-full compliance" membership category called "Associate Membership" beginning in 2002. The associate members of the NAI were allowed to be members of the NAI. However, associate members of the NAI were not required to

[66] BM 2007, Panel discussion, *Is Privacy the Third Rail*? July 24 2007. Video: <http://www.brightcove.tv/title.jsp?title=1126051143&channel=429048905>.

comply with the NAI principles. In 2005 and 2006, the associate members outnumbered the full members. (See Figure 4).

The associate membership category was not part of the original NAI agreement, and its existence seems violative of the spirit if not the letter of the agreement. Appendix A includes a complete listing of Associate and full NAI members over time. The category of associate membership was apparently abandoned in 2007, with no explanation given.

It is both noteworthy and disturbing that TRUSTe – the NAI external enforcement mechanism – was allowed to become an associate member of the NAI for one year, in 2005. TRUSTe should not have been a member of the organization for which it provides enforcement. It is hard to understand why TRUSTe sought and why NAI allowed TRUSTe to become a member. Even though the membership lasted for only one year, it undermines TRUSTe's supposed status as a neutral, independent overseer.

For a self-regulatory body whose purpose was to represent the network advertisers, NAI did not capture the membership it needed to be an effective, viable self-regulatory body. In addition, the creation of a category of non-compliant "members" calls into question the bona fides of NAI as a serious self-regulatory organization.

The NAI Definition of PII is Not Up-to-Date

The current NAI definition of personally identifiable information (PII), crafted in the 1990s, grew out of a culture and an economy still largely rooted in thinking about physical assets. Today, the economic structure prevailing in the U.S. increasingly embodies intangibles such as information and ideas. The definition of PII needs to move with the times. PII must expand beyond overly identifiable information and must include intangibles such as repeated online behavior that can be linked to a particular consumer.

The NAI currently defines PII as follows:

> Personally Identifiable Information (PII) is data used to identify, contact or locate a person, including name, address, telephone number, or email address.[67]

A more complete, modern definition of PII includes information that can directly or indirectly identify a person, and includes behavioral identifications:

> **Personally Identifiable Information** — Personally identifiable information (PII) consists of any information that can, directly or indirectly:
>
> (1) identify an individual, including but not limited to name, address, IP address, SSN and/or other assigned identifier, or a combination of unique or non-unique

[67] NAI FAQs, *What is personally identifiable information*? <http://www.networkadvertising.org/managing/faqs.asp>.

> identifying elements associated with a particular individual or that can be reasonably associated with particular individual, or
>
> (2) permit a set of behaviors or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier. Any set of actions and behaviors of an individual, if those actions create a uniquely identified being, is considered PII because the associated behavioral record can have tracking and/or targeting consequences.[68]

The point is that consumer tracking can be accomplished in the absence of traditional overt identifiers such as name and address. It does not matter if a consumer's name is known when that consumer's information is used to present offers and opportunities, to establish a price for a product or service, or to otherwise make decisions about a specific consumer. The presence or absence of an overt identifier when these decisions are made is irrelevant when consumers are individually tracked.

Given that much depends on the definition of PII, the NAI cannot be an effective consumer protection instrument until the definition of PII is updated to reflect current thinking and practices and to provide consumers with fair treatment. Hiding behind an outmoded definition of PII only contributes more to the irrelevancy of NAI today.

Notice: Still Not Clear or Conspicuous

One of the issues raised in the FTC reports to Congress about online behavioral profiling was notice. The FTC and the NAI promised "robust" enforcement of notice. Unfortunately, because the foundational understandings of the NAI are out of date, the NAI ideas of notice that flow from those understandings are also out of date.

Roy Shkedi, the founder and CEO of Almond Net, a behavioral advertiser, said the following at a Media Post conference:

> The consumer is always one click away from opting out .... most behaviorally targeted ads, you have no idea you are being targeted .... to find out you are being targeted, unless you are really web savvy, is really problematic.[69]

Almond Net is worth discussing in the context of notice because this company brands each targeted ads with the Almond Net name (Powered by Almond Net) and offers a one-click opt-out. This is a simple way of providing greatly increased notice in context. Privacy policies remain important. However, clicking through a privacy policy is not

---

[68] Consensus document filed with the FTC for the Nov. 1-2, 2007 Workshop, *Consumer Rights and Protections in the Behavioral Advertising Sector*.
<http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf >.

[69] Roy Shkedi, CEO of AlmondNet, *Is Privacy the Third Rail*?
<http://www.brightcove.tv/title.jsp?title=1126051143&channel=429048905>.

always possible or practical in newer advertising models, such as ads delivered to the mobile web. Does a seven-page privacy notice work on a mobile phone? However, branding on the face of delivered ads discloses where that ad originates and provides a consumer with a chance to figure out what is happening on the consumer's device.

In terms of notice, one of the great failures of the NAI is that technologies beyond the traditional cookie and web beacon or pixel tag are not required to be exposed to consumers. Notice is not required for new technologies such as Flash cookies or cache cookies.

Notice and Disabilities

Another NAI shortcoming is the failure to incorporate specific tools to assist individuals with disabilities. This was a mistake at the time the NAI agreement was published in 2000. But now, as the advertising technologies have become more sophisticated and have moved to additional devices, the situation is even more pressing.

Enforcement of NAI a Failure

The NAI agreement required NAI to either work with a third party enforcement program or undergo and publish regular compliance audits. In the FTC's second report to Congress on online profiling in which it recommended the NAI self-regulatory scheme, the FTC said:

> **The bedrock of any effective self-regulatory or legislative scheme is enforcement.** In a self- regulatory context, this means that nearly all industry members subject themselves to monitoring for compliance by an independent third party and to sanctions for non-compliance, which may include public reporting of violations or referral to the FTC. Enforcement may be provided by a seal organization, such as BBBOnline or TRUSTe. Under the NAI Principles, network advertisers have committed to working with an independent third party enforcement program (*e.g.*, a seal program) to ensure compliance with the Principles. If no such program is available within six months, the NAI companies will submit to independent compliance audits the results of which will be made publicly available.[70] (Emphasis added.)

Time has shown that enforcement of the NAI is inconsistent, opaque, and generally problematic.

NAI tasked TRUSTe with enforcement and oversight:

> **The NAI 3rd party enforcement program**

[70] See FTC *Online Profiling: A Report to Congress Part 2* at 8.

> The NAI and its member ad networks have engaged TRUSTe, a leading online privacy auditor, to manage an independent program that ensures compliance with the NAI self-regulatory principles. You can register complaints alleging non-compliance with the NAI Principles at this Website: http://www.truste.org/consumers/watchdog_complaint.php
>
> TRUSTe will investigate complaints via its Watchdog site. This process is managed entirely by TRUSTe and is completely independent of the NAI and its member ad networks.[71]

The official NAI site as of October 2007 still lists TRUSTe as its third party enforcement tool.[72]

TRUSTe's Systematic March From NAI Transparency

TRUSTe began reporting on NAI complaints in March 2002. It used its Watchdog Reports to do this. In the intervening years, TRUSTe public reports regarding the NAI reveal a troubling, systematic reduction of transparency regarding the NAI. (See Appendix B for a complete listing of all TRUSTe NAI complaints.)

In its first stage of reporting, for 10 months from March 2002 to December 2002, TRUSTe reported the total number of incoming NAI complaints, and it segmented those incoming complaints by grouping complaints about opt-out cookies and complaints about online preference marketing, among some other categories. (See Figure 5.) The resolution of NAI complaints was also included in the Watchdog Reports. So for example, in March 2002 anyone could see that 30 NAI complaints came in, and 30 of the complaints were about opt-out cookies. While this is not highly granular reporting, this reporting at least gave the public an ability to monitor what complaints were coming in, and in what areas.

[71] Network Advertising Initiative web site <http://www.networkadvertising.org/managing/enforcement.asp>. Last visited October 30, 2007.
[72] See <http://www.networkadvertising.org/managing/enforcement.asp>.

Watchdog Report for March 2002

Total Watchdog disputes received for the month:	404
Total Watchdog disputes received concerning valid TRUSTe sites:	278
Total privacy related Watchdog disputes received concerning valid TRUSTe sites:	181
Network Advertising Initiative (NAI) related disputes:	30
[1] Watchdogs Closed from March:	196
Watchdogs Closed from Previous Months:	27
Watchdogs Pending from March:	5
Privacy Related Issues:	
Unable to Un-subscribe	41
Received Spam	56
Felt PII was Shared Improperly	8
Felt Site was not Following Privacy Policy	4
Needed to Change PII	2
Wanted Account Closed and/or PII Deleted	28
Network Advertising Initiative - Opt-out Cookie	30
Network Advertising Initiative - Other Online Preference Marketing Related Issues	0
Other Privacy Concerns	42

Figure 5: a screenshot of the March 2002 report of 30 NAI opt-out cookie complaints. Note that incoming complaints are monitored. (Highlighting added for emphasis)

In the second stage of TRUSTe's NAI reporting, beginning January 2003, TRUSTe stopped reporting on any ***incoming*** NAI complaints. For a period of 24 months, from January 2003 – December 2004, TRUSTe only reported on the total number of NAI complaints that were ***resolved***, thus reducing the transparency of the reporting. (See Figure 6). TRUSTe still reported on how many opt-out cookie and OPM complaints were ***resolved***. But there was no more information on ***incoming*** complaints. This was an inappropriate step away from transparency.

Watchdog Report for December 2003

Total Watchdog disputes received for the month:		167
Total Watchdog disputes received concerning valid TRUSTe sites:		154
Total privacy related Watchdog disputes received concerning valid TRUSTe sites:		130
Network Advertising Initiative (NAI) related disputes:	2	
Watchdogs Closed from December:		117
Watchdogs Closed from Previous Months:		9
Watchdogs Pending from Previous Months:		15
Privacy Related Issues Resolved in December:		
Unable to Un-subscribe		15
Received Spam		19
Felt PII was Shared Improperly		14
Felt Site was not Following Privacy Policy		31
Needed to Change PII		8
Wanted Account Closed and/or PII Deleted		13
Children's Information (under 13)		0
Network Advertising Initiative - Opt-out Cookie		1
Network Advertising Initiative - Other Online Preference Marketing Related Issues		16
Other Privacy Concerns		

Figure 6: A screenshot of the December 2004 TRUSTe reporting format. Note that complaints are of privacy issues resolved. (Highlighting added for emphasis)

TRUSTe's reporting continued to devolve toward less transparency. In its third NAI reporting stage, beginning in January 2005 (TRUSTe became a member of the NAI organization in 2005 for a period of one year) and continuing until August of 2006, TRUSTe stopped reporting on anything other than the total number of NAI disputes that were resolved. (See Figure 7). For a period of 20 months, TRUSTe did no more reporting on incoming disputes, no more reporting on opt-out cookie complaints, and no more reporting on NAI OPM complaints.

Watchdog Report for November 2005

Total Watchdog disputes received for the month:	392
Total Watchdog disputes received concerning valid TRUSTe sites:	334
Total privacy related Watchdog disputes received concerning valid TRUSTe sites:	317
Total Watchdog complaints that were closed for the month:	392
Privacy Related Issues Resolved in November:	
Undefined	65
Unable to Unsubscribe	41
Felt PII was Shared Improperly	2
Unable to change personal information	8
Unable to close account	30
Email sent without permission	1
Unwanted email	1
Phishing	9
Spyware	5
Transactional/Monetary/Billing	36
Account Access/Account Creation/Password Issue	72
Unauthorized Profile with My Information	3
Network Advertising Initiative (NAI) related disputes	72
Public Abuse	21
Other	26

Figure 7: TRUSTe begins reporting only the total NAI privacy issues resolved (2005-August 2006). (Highlighting added for emphasis)

Then finally, in September 2006 until the current time, TRUSTe no longer reports publicly on the NAI complaints whatsoever in its Watchdog Reports. There is no longer any category available in the TRUSTe Watchdog Reports for NAI-related complaints. It is unknown why TRUSTe moved systematically stepwise away from transparency, but the Watchdog Reports speak for themselves.

Watchdog Report for September 2006

Total Watchdog disputes received for the month:	253
Total licensee complaints filed during period - privacy related (TRUSTe Diagnosis)	57
Total Watchdog complaints that were closed for the month:	239
Privacy related issues: TRUSTe Diagnosis	
Unable to Unsubscribe	25
Received email spam	1
Email sent without permission	12
Unwanted email	1
Shared personal information	2
Unable to close account	13
Unable to contact licensee	1
Unauthorized Profile with My Information	2
TOTAL	57

Figure 8: Screenshot of TRUSTe's current report format. There is no specific reporting about the NAI in the WatchDog reports.

It is implausible to think that NAI complaints ceased, and there was nothing to report. From March 2002 to August 2006, the last month that TRUSTe reported NAI complaints, each and every month's Watchdog Reports listed NAI complaints that had been received, save for one month. In December 2005 there were 66 NAI disputes. Are we to believe that in December of 2006, one year later, there were zero disputes and that is why the category was omitted entirely? After nearly 5 years of monthly NAI complaints, it seems unlikely that the NAI complaints evaporated without a trace. Even if that were the case, TRUSTe could have reported zero complaints.

Appendix B lists the complete public history of the NAI complaints as handled by TRUSTe.

Is TRUSTe Really Independent?

It is difficult to reconcile the statement of the NAI that TRUSTe is an independent enforcement program, when TRUSTe was a member of the organization it was the enforcement mechanism for in 2005. It is wholly inappropriate for an independent overseer to be a member of an organization that it is overseeing.

Where Are the Audits?

The NAI agreement states that either the member organizations must submit to an independent seal program that conducts random audits, or they must undergo independent audits. There is no information showing whether TRUSTe actually conducted random audits.

If TRUSTe conducts independent audits of NAI members, an auditing methodology should be published for transparency. Nothing is known about auditing by TRUSTe, and the lack of information undermines the credibility of both TRUSTe and NAI. Nothing on the public record suggests that TRUSTe actually conducted any of the required audits.

Enforcement of NAI Sensitive Data Safeguards

The NAI agreement contains language that restrict NAI members from using certain types of information:

> Sensitive Data: Network advertisers shall neither use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, nor social security numbers for [Online Preference Marketing].[73]

It is not clear how NAI members implement this limitation. First, what constitutes sensitive medical information? Some may believe that any information about health care constitutes sensitive medical information. Others may believe that the only sensitive medical information relates to HIV/AIDS, drug treatment, or issues related to mental health. Because the NAI agreement did not specify what constituted sensitive medical information, each company can decide for itself.

For example, Tacoda, in a press release announcing its Consumer Choice Initiative, noted, "Tacoda will avoid targeting advertisements using sensitive data, such as sexual preference, certain medical conditions, or identifying children. Current industry practices permit targeting on this type of data."[74] What are "certain medical conditions"? Why do current industry practices allow targeting using types of data that appear to be expressly prohibited in the NAI agreement? If current industry practices permit targeting on this data, then the current industry practices have apparently not been touched by the NAI.

When NAI standards are unclear, it is impossible to hold members or the NAI accountable for compliance. This may account, in part, for the lack of audit information from TRUSTe.

Oversight of NAI is a Failure

Oversight of the NAI has been neglected. As a result, there are many things the public simply does not know about the program, in particular, its effectiveness. To date, the public does not know how many consumers participate in the program. The public does not have numbers comparing consumers who have visited opt-out pages with consumers who have successfully opted out. How many consumers actually have opt-out cookies, and for how long? Where are the reports on whether or not it is effective for those who do opt-out? Are NAI members actually complying with the obligations?

The scant information available from the TRUSTe watchdog reports indicated a steady history of consumer complaints about the NAI, at least until the information was suppressed altogether. Which companies and/or sites received complaints? What happened? These are the kinds of questions a solid oversight program would answer.

What consumers are left with are many more questions than answers and information, and this is a hardly a hallmark of an effective, thorough oversight program.

---

[73] See *Network Advertising Initiative, Self-regulatory Principles for Online Preference Marketing by Network Advertisers*, July 10, 2000. < http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf>.

[74] Market Wire, Press Release. *Tacoda Launches Consumer Choice Initiative; Plans Consumer Opt-Out Preservation with New Patent-Pending Technology*, November 6, 2006.

Conclusion

The NAI has failed. The agreement is foundationally flawed in its approach to what *online* means and in its choice of the opt-out cookie as a core feature. The NAI opt-out does not work consistently and fails to work at all far too often. Further, the opt-out is counter-intuitive, difficult to accomplish, easily deleted by consumers, and easily circumvented. The NAI opt-out was never a great idea, and time has shown both that consumers have not embraced it and that companies can easily evade its purpose.

The original NAI agreement has increasingly limited applicability to today's tracking and identification techniques. Secret cache cookies, Flash cookies, cookie re-setting techniques, hidden UserData files, Silverlight cookies and other technologies and techniques can be used to circumvent the narrow confines of the NAI agreement. Some of these techniques, Flash cookies in particular, are in widespread use already. These persistent identifiers are not transparent to consumers. The very point of the NAI self-regulation was to make the invisible visible to consumers so there would be a fair balance between consumer interests and industry interests. NAI has not maintained transparency as promised.

The behavioral targeting industry did not embrace its own self-regulation. At no time does it appear that a majority of behavioral targeters belong to NAI. For two years, the NAI had only two members. In 2007 with the scheduling of the FTC's new Town Hall meeting on the subject, several companies joined NAI or announced an intention to join. Basically, the industry appears interested in supporting or giving the appearance of supporting self-regulation only when alternatives are under consideration.

Enforcement of the NAI has been similarly troubled. The organization tasked with enforcing the NAI was allowed to become a member of the NAI for one year. This decision reveals poor judgment on the part of the NAI and on the part of TRUSTe, the NAI enforcement organization. Further, the reporting of enforcement has been increasingly opaque as TRUSTe takes systematic steps away from transparent reporting on the NAI. If the enforcement of the NAI is neither independent nor transparent, then how can anyone determine if the NAI is an effective self-regulatory scheme?

The result of all of these and other deficiencies is that the protections promised to consumers have not been realized. The NAI self-regulatory agreement has failed to meet the goals it has stated, and it has failed to meet the expectations and goals the FTC laid out for it. The NAI has failed to deliver on its promises to consumers.

Credits:

Author: Pam Dixon, executive director, World Privacy Forum

Editor: Robert Gellman

Graphics: John Boak

Technical review: The World Privacy Forum thanks the individuals who contributed to the technical review of this report.

For More Information:

PDF version of this report is located at
<http://www.worldprivacyforum.org/pdf/WPF_NAI_report_11022007>.

For More Information Contact:

World Privacy Forum
760-436-2489
www.worldprivacyforum.org

Appendix A: List of NAI Members (all categories) 1999-2007

To compile this list, the World Privacy Forum relied on saved pages of NAI available on Archive.org.

NAI membership from 1999- 2007

November 1999	November 2000	November 2001	November 2002
24/7 Media AdForce AdKnowledge Adsmart DoubleClick Engage Flycast MatchLogic NetGravity (a division of DoubleClick) Real Media *No associate members listed*	24/7 Media AdForce AdKnowledge Adsmart Avenue A Burst! Media DoubleClick Engage Flycast MatchLogic NetGravity (a division of DoubleClick) Real Media *No associate members listed*	Avenue A DoubleClick L90 Matchlogic(suspended Sept. 24th) 24/7 Media *No associate members listed*	Avenue A DoubleClick *Three associate members listed:* *L90* *24/7* *ValueClick*
November 2003	November 2004	November 2005	November 2006
Atlas DMT Doubleclick *Two associate members listed:* *24/7* *ValueClick*	Atlas DMT Doubleclick Tacoda Systems Inc. 24/7 Real Media *Two associate members listed:* *ValueClick* *WebSideStory*	Atlas BehaviorLink Doubleclick Poindexter Systems Revenue Science Tacoda 24/7 RealMedia *17 associate members listed :* *Adteractive* *AlmondNet* *America Online* *AWS*	Advertising.com, Inc. Atlas DoubleClick [x+1] (formerly Poindexter Systems, Inc.) Revenue Science, Inc. SpecificMEDIA, Inc. TACODA, Inc. 24/7 Real Media Inc. 17 associate members listed in 2 categories: *121 Media* *Adteractive*

		Casale Media *Direct Revenue* *Exact Advertising LLC* *Fastclick* *Hotbar.com Inc* *IAB* *Intermix Media* *180Solutions* *TRUSTe* *ValueClick* *WAA* *WebSideStory* *WhenU*	*AlmondNet* *America Online, Inc.* *BlackFoot, Inc.* *Casale Media, Inc.* *Claria Corporation* *Contextweb, Inc.* *Fastclick* *ValueClick, Inc.* *The following companies are members in-good-standing with the NAI* *AWS* *Direct Revenue, LLC* *eXact Advertising, LLC* *Hotbar, Inc* *Intermix Media, Inc.* *WhenU* *Zango, Inc.*
May 2007 Advertising.com, Inc. Atlas DoubleClick [x+1] Revenue Science, Inc. SpecificMEDIA, Inc. TACODA, Inc. 24/7 Real Media Inc. No associate members listed			

2007 NAI Membership Activity

May 2007	August 2007
Advertising.com, Inc.	Acerno

Atlas DoubleClick [x+1] Revenue Science, Inc. SpecificMEDIA, Inc. TACODA, Inc. 24/7 Real Media Inc.	AlmondNet Advertising.com, Inc. Atlas DoubleClick [x+1] Revenue Science, Inc. SpecificMEDIA, Inc. TACODA, Inc. 24/7 Real Media Inc.

Appendix B: Listing of TRUSTe Complaints Regarding NAI From 2000 – 2007

Note: The World Privacy Forum relied on the TRUSTe WatchDog reports to compile this table. For the reports, see: <http://www.truste.org/consumers/watchdog_reports.php>.

2007

Sept. No mention of NAI
Aug. No mention of NAI
July No mention of NAI
June No mention of NAI
May No mention of NAI
April No mention of NAI
March No mention of NAI
Feb. No mention of NAI
Jan. No mention of NAI

2006

Dec. No mention of NAI
Nov. No mention of NAI
Oct. No mention of NAI
Sept. No mention of NAI
Aug. **Last noted mention of NAI in WatchDog reports**: 3 NAI disputes
July 7 NAI disputes
June 3 NAI disputes
May 9 NAI disputes
April 2 NAI disputes
March 4 NAI disputes
Feb. 3 NAI disputes
Jan. 5 NAI disputes

2005

Dec. 66 NAI disputes
Nov. 72 NAI disputes
Oct. 10 NAI disputes
Sept. 9 NAI disputes
Aug. 5 NAI disputes
July 10 NAI disputes
June 18 NAI disputes
May 33 NAI disputes
April 8 NAI disputes
March 6 NAI disputes
Feb. 14 NAI disputes
Jan. 18 NAI disputes (No more disclosure of Opt-out cookie or OPM after this date.)

2004

Dec. 16 NAI disputes resolved: 10 opt-out cookies, 2 OPM
Nov. 9 NAI disputes resolved: 7 opt-out cookies, 1 OPM
Oct. 6 NAI disputes resolved: 3 opt-out cookies, 1 OPM
Sept. 12 NAI resolved 4 opt out cookie, 2 OPM
Aug. 17 NAI disputes resolved: 7 opt-out cookies 5 OPM
July 6 NAI disputes resolved: 3 opt-out cookies, 2 OPM
June 4 NAI disputes resolved: 2 opt-out cookies, 1 OPM
May 7 NAI disputes resolved: 3 opt-out cookies
April 1 NAI disputes resolved: 1 opt-out cookie
March 5 NAI disputes resolved: 2 opt-out cookies, 1 OPM
Feb. 6 NAI disputes resolved: 4 opt-out cookies
Jan. 8 NAI disputes resolved: 2 opt-out cookies, 3 OPM.

2003

Dec. 2 NAI disputes resolved: 1 opt-out cookie, 16 OPM
Nov. 8 NAI disputes resolved: 4 opt-out cookies 1 OPM
Oct. 4 NAI disputes resolved: 1 opt-out cookie, 2 OPM
Sept. 2 NAI disputes resolved: 1 opt-out cookie
Aug. 2 NAI disputes resolved 1 opt-out cookie
July 5 NAI disputes resolved: 3 opt-out cookies
June 4 NAI disputes resolved: 2 opt-out cookies
May 5 NAI disputes resolved: 2 opt-out cookies 1 OPM
April 4 NAI disputes resolved: 1 opt-out cookie 1 OPM
March 1 NAI disputes resolved: 1 opt-out cookie
Feb. 3 NAI disputes resolved: 1 opt-out cookie 1 OPM
Jan. 4 NAI disputes resolved: 1 opt-out cookie

2002

Dec. 1 NAI dispute
Nov. 0
Oct. 1 NAI dispute
Sept. 1 NAI dispute
Aug. 4 NAI disputes
July 7 NAI disputes
June 5 NAI disputes involving 5 opt-out cookies
May 4 NAI disputes involving 4 opt-out cookies
April 7 NAI disputes involving 7 opt-out cookies
March 30 NAI disputes involving 30 opt-out cookies