Comments of

Professor Peter P. Swire
Moritz College of Law, The Ohio State University
Senior Fellow, Center for American Progress

and

Professor Annie I. Antón
Computer Science Department
College of Engineering
North Carolina State University

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

April 10, 2008

Executive Summary

These comments are submitted jointly by a law professor and computer science professor to address key technical issues in online behavioral profiling.

The Federal Trade Commission has asked for comments on its Proposed Self-Regulatory Principles for Online Behavioral Advertising. The first principle is "transparency and consumer control." The essence of "consumer control," under the proposed principle, is that consumers "can choose whether or not to have their information collected for such purpose."

These comments examine what technical steps are needed to implement the Consumer Control Principle. The comments do not take any position on whether this principle of consumer control should become part of a self-regulatory or regulatory system.

Our principle findings are the following:

1. Cookies, as flawed as they are, are the primary existing mechanism for a website to determine that the same computer (or similar device) is returning to the website. We thus propose mechanisms for making cookies much more effective at upholding consumer choice with respect to behavioral targeting. Although "opt-in" cookies are technically feasible, we assume that the current policy discussion concerns "opt-out cookies," which support consumers who choose not to participate in behavioral profiling.

2. Opt-out cookies today are often deleted by anti-spyware software. We recommend that anti-spyware software should be modified to honor opt-out cookies. It is technically feasible to create standards for opt-out cookies, and we believe security risks can be effectively addressed through creation of a public "white list" of opt-out cookies that will not be used for tracking.

3. Similarly, opt-out cookies are often deleted today when consumers use their browser software to delete *all* cookies. We recommend that browser software be updated to manage opt-out cookies better. As with anti-spyware software, the standards and security issues appear manageable.

In short, modest steps for anti-spyware and browser software can make opt-out cookies a much more effective tool for consumer choice about behavioral profiling. Unless these or similar technical measures are taken, the proposed FTC Consumer Control Principle will fail. Consumers will lack a feasible way to exercise their choice.

Introduction

We thank the Federal Trade Commission for the opportunity to comment on "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles." In these comments, we first briefly describe the relevant background of the co-authors. We discuss the Consumer Control Principle, and explain why opt-out cookies, as imperfect as they are, are the principle current technology for exercising consumer choice about behavioral profiling. We then examine how anti-spyware and browser software currently create important difficulties for the use of opt-out cookies, and recommend technical measures that would address these difficulties.[1]

Background of the Co-Authors

Peter P. Swire is the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. He is also Senior Fellow at the Center for American Progress. From 1999 until early 2001, he served as Chief Counselor for Privacy, in the U.S. Office of Management and Budget. Among his other activities in that role, he worked on issues of behavioral advertising that culminated in creation of the Network Advertising Initiative. More recently, he was an invited participant for the FTC's examination of behavioral profiling and related issues in "Protecting Consumers in the Next Tech-Ade," in 2006, and the Town Hall on "Ehavioral Advertising: Tracking, Targeting, and Technology," in 2007. His publications are available at www.peterswire.net.

Annie I. Antón is an Associate Professor of Software Engineering in the College of Engineering at the North Carolina State University. She joined the computer science department at NC State in 1998. From 2005-2006 she was a visiting faculty (sabbatical) scholar at Purdue University's CERIAS. She is the founder and director of ThePrivacyPlace.Org, currently chairs the 2008 NC State Public Policy Task Force, and is Co-Chair of the U.S. Association of Computing Machinery Public Policy Committee's Privacy Subcommittee. Antón currently serves on various boards, including: the National Science Foundation Computer & Information Science & Engineering Directorate Advisory Council, the Department of Homeland Security Data Privacy and Integrity Advisory Committee, and the Computing Research Association Board of Directors. Her publications are available at: www.csc.ncsu.edu/faculty/anton.

The Consumer Control Principle

This testimony focuses on technical issues arising from the Federal Trade Commission's first proposed principle, on "transparency and consumer control":

> "Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option."

The essence of "consumer control," under the proposed principle, is that consumers "can choose whether or not to have their information collected for such purpose." There should be "a clear, easy-to-use, and accessible method for exercising this option."

This testimony examines the technical steps that need to be taken to implement the Consumer Control Principle. Unless the technical infrastructure is in place, there will be no "easy-to-use and accessible" method for exercising consumer choice. This testimony does not take any position on whether this principle of consumer control should become part of a self-regulatory or regulatory system.[2]

The Consumer Control Principle does not specify whether consumer choice should be opt-out (behavioral profiling happens unless the user opts out) or opt-in (behavioral profiling happens only after a user opts in). Consistent with the focus of this testimony on technical issues, this testimony takes no position on whether choice would be opt-out or opt-in, but we assume that the policy discussions are focused on opt-out approaches. The technical issues for either approach would be much the same—what mechanisms exist for a website or advertising network to recognize the same computer or other device as the same.

Cookies as the Central Existing Technology for Consumer Choice

This testimony is based on the assumption that cookies are the primary existing mechanism for a website to determine that the same computer (or similar device) is returning to the website.[3] In terms of the Consumer Control Principle, the website must have a mechanism for knowing that a user has allowed or disallowed behavioral profiling. This testimony proposes mechanisms for making cookies effective at upholding consumer choice with respect to behavioral targeting.

Session and Persistent Cookies

We recognize, as discussed below, that cookies are a quite imperfect mechanism for exercising consumer choice. For the reasons explained here, we nonetheless believe that fixing cookies, especially through an improved system for opt-out cookies, is a workable and promising path for improving consumer choice.

The basic virtue of cookies is that they allow a website to recognize the same computer when it returns to the website. Some cookies are "session" cookies, which allow the website to recognize the same user for as long as the user's browser remains open. These session cookies are useful, for instance, for online shopping carts—the session cookie enables the website to take the user through a series of screens, from product display through ultimate purchase. When an expiration date is not specified, session cookies are deleted each time the browser is closed.

Other cookies are "persistent" cookies, which allow the website to recognize the same computer on later visits, up until the date the cookie expires. Persistent cookies have historically been the subject of privacy concern due to the possibility that web surfing will be tracked in ways that consumers may not understand or desire. Responses to privacy concerns about persistent cookies have included:

1. Guidance from the Office of Management and Budget in 2000 concerning persistent cookies on federal websites.[4]
2. The Network Advertising Initiative principles promulgated in 2001, including use of opt-out cookies for third-party advertising networks.[5]
3. Inclusion in major browsers of settings for users to manage cookies, including defaults that limit the use of many third-party cookies.

Along with the privacy concerns reflected in these measures, persistent cookies have also become widespread in many online commercial settings. Notably, persistent cookies are an important feature in many or most systems for online behavioral targeting. Although the technical details vary, websites typically rely on persistent cookies to identity the same computer. They then can select content or advertisements based on the web activities of that same computer—the essence of online behavioral targeting.

Opt-Out Cookies to Date

The central technical challenge for the Consumer Control Principle is how the consumer can signal an ongoing desire not to be subject to behavioral targeting. As already explained, there is a standard technology on the Web for identifying the same computer when it visits a website—the cookie. This feature, of identifying the same computer, has given rise to the "opt-out cookie."

An opt-out cookie indicates that the user of a particular computer wants to opt out of something—wants the website to recognize the user's choice during repeated visits to the site. Under the NAI Principles, members of NAI have an opt-out cookie linked from the NAI and other websites. NAI members promise not to use targeting to advertise to those computers that have the opt-out cookie.

There are various technical and practical objections to relying on opt-out cookies. One of the biggest problems, and the focus of this testimony, is the need for changes to anti-spyware and browser software to reduce greatly the number of opt-out cookies that are presently deleted. In brief, here are some of the objections that have been raised to reliance on opt-out cookies:

1. *Opt-out cookies are still cookies.* It may seem counter-intuitive to rely on a technology that is often called privacy-threatening (cookies) in order to implement privacy preferences. The basic answer to this objection is to ask for a better alternative. Because cookies are the already-deployed way to retain state (to recognize a returning computer as the same), then opt-out cookies are the logical way to retain state for consumer choice about behavioral targeting. This feature of opt-out cookies is presumably why they were incorporated into the previous round of responses to issues of online behavioral advertising, as reflected in the NAI Principles.

2. *Opt-out cookies do not work in some computer environments.* The World Privacy Forum has documented how some firewalls and other system configurations sometimes defeat a user's attempt to set an opt-out cookie.[6] Its report recommended that "it would be appropriate for NAI to provide detailed assistance on its website that reflects the variety and complexities of Internet usage." This area deserves further research into what sorts of

technical settings create obstacles to setting opt-out cookies, how best to promulgate information about best practices, and who is in the best position to make consumer choice effective.

3. *Opt-out cookies are confusing to consumers.* It is certainly true today that few Internet users have a good understanding of cookies,[7] much less opt-out cookies. There is survey evidence that users often lack understanding about how to manage ordinary persistent cookies.[8] Opt-out cookies are less well-known than ordinary cookies, so it is almost certain that consumers understand them less well. This problem of consumer confusion is a reason to expect consumer education to be a prominent part of any implementation of the Consumer Control Principle. Reduction in consumer confusion can result from improved software design, so that consumers can easily indicate their choice. Thoughtful choice of defaults in software also can reduce consumer confusion, so that there is "privacy by design" in appropriate settings.[9]

These and other possible criticisms of opt-out cookies should be taken seriously. If comments to the FTC show other technical mechanisms for implementing the Consumer Control Principle, then the Commission may wish to encourage those other mechanisms.[10] We have reached the tentative conclusion, however, that opt-out cookies—imperfect as they are—are the most plausible technology currently and widely available for implementing the Consumer Control Principle.[11] Therefore, we now turn to technical measures that would allow opt-out cookies to function more effectively than they do today.

Opt-Out Cookies and Anti-Spyware Software

Many current opt-out cookies are deleted by anti-spyware software. This section of the testimony explains the problem and manageable steps that would address the problem.

A simple example illustrates the problem. Suppose a consumer on Monday sets an opt-out cookie with the NAI or at another website. On Tuesday, the consumer's anti-spyware software might do its regular check on the consumer's computer, and delete the opt-out cookie along with all other cookies on the computer. On Wednesday, therefore, the opt-out cookie would have been deleted, and the consumer would be subject to behavioral targeting once again. The reason that anti-spyware deletes opt-out cookies is that it is not interpreting (and in general cannot interpret) the content of the cookies, it is merely deleting *all* cookies from sites not known to be "benign."

Our basic point is that anti-spyware software should be modified to honor opt-out cookies. In the example, the software would do its check on Tuesday, but the opt-out cookie would remain in place. The consumer's choice would thus be implemented.[12]

One of the authors proposed this approach during a presentation at a Public Meeting of the Anti-Spyware Coalition in January, 2008.[13] The off-the-record responses from industry were positive, including statements by some that it would not be expensive or technically difficult to implement. However, two questions were raised about how to write anti-spyware software so that opt-out cookies would remain in place—standards and security.

Standards for Opt-Out Cookies

In order for anti-spyware companies to recognize opt-out cookies, there must be criteria or standards for defining an "opt-out cookie." Based on discussions with experts in the field, the technical aspects of such standards do not appear difficult. A more difficult question, discussed below, is how to enforce against those who try to abuse the standards. Support from vendors of anti-spyware software would be very helpful for creating such standards.

Security and Opt-Out Cookies

The other question is whether there are any security risks created by anti-spyware companies recognizing opt-out cookies. In general, the security risks associated with cookies are low, because cookies are written into a text file and no code is executed.[14]

The biggest risk that we have identified is that other sorts of cookies might get disguised as opt-out cookies in order to avoid being deleted by anti-spyware software. The concern is that a persistent cookie might be written in a form that meets the standard for opt-out cookies, but instead be used by a website or ad server as tracking cookies.

There is no simple technical measure that would prevent this deceptive use of tracking cookies. In response to this concern, we tentatively recommend that a public white list be developed for opt-out cookies. The white list could include the name of the company setting the opt-out cookies, and it would be helpful to have an email address or other informed point of contact if there are questions or complaints. Only opt-out cookies on the white list would be recognized by anti-spyware software. An advantage of this sort of white list is that the organizations on the white list would be making public statements that the opt-out cookies are not being used for tracking. Using the opt-out cookies for tracking would thus be a deceptive practice, enforceable by the FTC under its Section 5 authority.

If such a white list were developed, then it could be housed in either the public or private sector. A precedent for the public sector is the list maintained by the U.S. Department of Commerce for companies that have signed up for the privacy Safe Harbor with the European Union. White lists can also be maintained by private or self-regulatory organizations. We do not take a position on how to maintain the white list, but instead underscore that use of a white list, and enforcement against violators, would strengthen operation of opt-out cookies for consumer choice.

Opt-Out Cookies and Browser Software

A second major source of deleted opt-out cookies is by individuals who use their browsers to delete their cookies, and thereby delete opt-out cookies. Once again, a simple example illustrates what happens. On Monday, the consumer opts out of behavioral tracking, and an opt-out cookie goes onto the computer. On Tuesday, the consumer deletes all cookies, perhaps after hearing that they create privacy problems. Opt-out cookies are deleted along with other cookies. On Wednesday, the consumer is again being tracked for purposes of behavioral targeting.

Our basic point for browsers is that the settings should be updated to handle opt-out cookies better. There are various possible ways to give users more granular control over cookies. Developers of browser software are in a better position than we are to decide the best way to implement this. But the basic idea is simple enough—it should be easy for users to set opt-out cookies, and to have the opt-out cookies remain in place when other cookies are deleted.

One possible direction for browser software is to modify the default. In this approach, when users decided to delete cookies, the default would delete other cookies but retain opt-out cookies. Users might then get a pop-up message saying something like: "You have cookies on your machine that indicate you choose not to be subject to tracking by the following sites: <show list of sites.> Do you wish to change that choice, so that the sites can now keep records of your browsing activities? Once again, we underscore that we are not trying to say the best way to develop browser software, and the language here only suggests one approach to wording the message. Instead, our goal is to explain the reasons that underlie our call to update browser software to handle opt-out cookies in a way that appropriately implements the FTC's Consumer Control Principle.

As with anti-spyware software, there are possible issues of standards for defining opt-out cookies and addressing security concerns. The answers for browser software are essentially the same on these topics as for anti-spyware software:

- For standards, it is desirable to have standards that work seamlessly across tracking systems. Notably, the same standards and the same white list should likely apply to anti-spyware software and browsers. In addition, if and as tracking technologies other than persistent cookies are used, then the standards should extend to those additional technologies.
- For security, the white list should be accessible to developers of browser software. The goal, in order to meet the Consumer Control Principle, is to make actual user control simple, understandable and usable. It may make sense, therefore, for browser software to update regularly the list of opt-out cookies on the white list.

Conclusion

The goal of our comments is to address technical issues that need to be solved in order to achieve the proposed Consumer Control Principle for behavioral advertising. In essence, we are trying to make the principle work for consumers when they opt out. The vagaries of anti-spyware or browser software should not override this exercise of consumer choice. We hope that good-faith participants in the industry will work together to make the existing tools for choice substantially more effective.

There are broader questions to consider, as well. One large question is how consumers will be educated about the choices they have with respect to behavioral advertising. Another is the extent to which consumer choice about behavioral advertising should follow the pattern set for telemarketing. In telemarketing, there are company-specific Do Not Call lists, for consumers who do not wish to receive marketing calls from a particular company. The FTC has also, however, created the national Do Not Call registry, for the consumers who have decided to opt

out of home telemarketing calls more generally. From the point of view of consumer ease-of-use, the national Do Not Call registry has been a great success. Going forward, an important question for the FTC, industry, and public advocacy groups is how to build consumer ease-of-use and the Consumer Control Principle into the new technologies of the online advertising industry.

Endnotes

---

[1] We would like to acknowledge comments on earlier drafts from members of the U.S. ACM Public Policy Committee Executive Committee, including Ben Bederson, Jim Horning, and Gene Spafford.

[2] One of the authors published an article in November, 2007, calling for consumer choice along the lines of the FTC's proposed Consumer Control Principle. Peter Swire, "We Are the Web," Dec. 18, 2007, available at http://www.americanprogress.org/issues/2007/12/we_are_the_web.html . The point of the current testimony, however, is not to argue for or against such a principle, or take any position on that principle. Instead, this testimony examines the technical prerequisites of implementing the Consumer Control Principle.

[3] Kristol, D. M. 2001. HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology.* 1, 2 (Nov. 2001), pp. 151-198.

[4] www.whitehouse.gov/omb/memoranda/m00-13.html.

[5] www.networkadvertising.org.

[6] Pam Dixon, World Privacy Forum, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation," at 17 (2007), available at http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

[7] Ha, V., Inkpen, K., Al Shaar, F., and Hdeib, L. 2006. "An examination of user perception and misconception of internet cookies," in *CHI '06 Extended Abstracts on Human Factors in Computing Systems* (Montréal, Québec, Canada, April 22 - 27, 2006). CHI '06. ACM, New York, NY, pp. 833-838.

[8] Id. at 27.

[9] One example of the importance of defaults was the decision of Microsoft to set the default in Internet Explorer to refuse third-party cookies except in limited circumstances.

[10] Many possible mechanisms for implementing consumer choice about behavioral targeting would require measures that would likely be more privacy invasive and/or more cumbersome for consumers. For instance, a website could require surfers to identify themselves upon visiting the site, and targeted ads would only be served to consumers who had not opted out. This sort of identified surfing is less privacy protective than normal surfing practices today at websites. Another approach would be for websites to require a username and password for each visit to the site. Users who opted out would not be subject to behavioral targeting. The username could be a pseudonym, so the website would not necessarily know the surfer's identity. This approach, however, would be significantly more cumbersome for consumers than surfing at many sites today. Users would need to keep track of usernames and passwords for all of these sites, which many users would not like. In addition, users quite possibly would use one or a few

passwords at the many sites, raising security problems for users who select the same password for their high-value sites such as online banking.

[11] Our comments focus on the use of persistent cookies for web browsing, which is the major technique today and in the near future for behavioral profiling. Looking ahead, behavioral profiling technologies will likely develop so that other technical measures, beyond opt-out cookies, would be needed in order to achieve implementation of the Consumer Control Principle. For instance, the use of "flash" cookies does not today have effective choice mechanisms associated with it.

[12] There are significant advantages for having anti-spyware software recognize and honor legitimate opt-out cookies. Without preservation of these cookies, a website or advertising network may link a user to previous visits, even if the website's or advertising network's usual cookies are deleted periodically by anti-spyware software. The reason is that the website or advertising network may have other mechanisms for determining, on a probabilistic basis, that a static IP address or other feature of the device is likely to be the same device (or user) over time. Essentially, opt-out cookies indicate that the user does not want "re-linking"—the ability of the website or advertising network to continue with behavioral profiling even after a cookie is once deleted.

[13] http://www.peterswire.net/psspeeches2008.htm.

[14] There is one known security problem with cookies worth mentioning, but the proposed use of opt-out cookies would not seem to increase the risk from it. In some instances, cookies become a shortcut for spoofing of authentication systems. Malicious third parties in some instances can intercept cookies, allowing them to intercept the session between a user and a website. We do not believe that this risk is measurably changed by the use of opt-out cookies described in this testimony.