CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Applying the FTC's Spyware Principles to Behavioral Advertising

Comments of the Center for Democracy & Technology In regards to the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology"

October 19, 2007

The Center for Democracy & Technology (CDT) is pleased to have the opportunity to submit comments for the upcoming Federal Trade Commission Town Hall entitled "Ehavioral Advertising: Tracking, Targeting, and Technology." In the seven years that have passed since the FTC last explored the privacy implications of targeted online advertising, advances in technology and the evolution of business models have created an entirely new landscape that warrants renewed attention to this issue.

Introduction

Over the past several years, the FTC has taken the lead law enforcement role in fighting spyware, one of the most serious threats to the Internet's continued usefulness, stability and evolution. The Commission has brought a total of 11 spyware enforcement actions, and in doing so has played a key role in stemming the tide of this Internet scourge. In these comments, CDT will outline how the key principles of the Commission's spyware work can be applied in the behavioral advertising context.[1]

In the course of its spyware enforcement activities, the FTC has identified a set of guiding principles. As outlined by FTC Chairman Deborah Platt Majoras in her address at the Anti-Spyware Coalition public workshop in February 2006, the principles are as follows:

1. "A consumer's computer belongs to him or her . . .. Internet businesses are not free to help themselves to the resources of a consumer's computer."

2. "Buried disclosures do not work."

3. "If a distributor puts a program on a consumer's computer that the consumer does not want, the consumer should be able to uninstall or disable it."[2]

---

[1] In this document, "behavioral advertising" is defined as the practice of tracking consumers' activities online to target advertising, in accordance with the definition in the FTC's announcement for the Town Hall. See *Ehavioral Targeting: Tracking, Targeting, and Technology*, Federal Trade Commission, http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

[2] *Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission*, Anti-Spyware Coalition Public Workshop, Feb. 9, 2006, http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf.

These principles provide an appropriate framework for evaluating not just potential spyware activities, but behavioral advertising practices as well.

For one thing, in some cases spyware tactics and behavioral advertising practices can effectively be one and the same – because spyware is being used as a means to track consumers' Internet activity for the purpose of delivering targeted advertising. In several of its cases the FTC has focused on adware that surreptitiously tracks users' Internet activity and serves advertising based on the information collected. In the Enternet Media case, for example, the FTC took issue with software code that "tracks consumers' Internet activity," claiming that this practice formed part of an unfair act that was "likely to cause substantial injury to consumers."[3] In total, six out of the Commission's 11 spyware cases have dealt with the practice of tracking Internet activity for the purposes of serving advertising, and in two of those cases this tracking was considered part of an unfair act.

More broadly, the FTC's spyware principles revolve around the concept of user control – ensuring that consumers are in command of their computers, what gets stored on those computers, and how those computers can be accessed by Internet businesses. The FTC has not hesitated to act against a wide range of behaviors that jeopardize user control by violating these principles. The behaviors the agency has targeted to date all involve software programs – but, as discussed below, there are other technical means that can be used to achieve largely the same results, with similar disregard for the user's right to control his or her own computer. The importance of user control is not dependent on the specific technical method used for accessing a computer or tracking user behavior.

Of course, some of the Commission's spyware actions have targeted many other practices that have damaged consumers' computers or caused consumers to incur financial loss. CDT does not intend to equate all spyware practices with all behavioral advertising practices. Rather, by focusing on some of the common behaviors that underlie both – and the principles the FTC has developed to address these behaviors with regards to spyware – we hope to demonstrate that in the behavioral advertising context, no less than in the spyware context, harms may involve the loss of users' control over their computers and associated consequences of that loss, including but not limited to financial harms or damage to property. Because of this commonality, we believe that consumers deserve just as robust protections against unwanted behavioral tracking and targeting as the FTC has extended to them in the spyware space.

It is useful to consider an example behavioral advertising scenario in order to understand this conceptualization. Consider a user who is doing some Web browsing. As the user surfs the Web, his or her browser retains a history of recently viewed sites. The user can later refer to this list in order to quickly return to these sites. In recent years, several different researchers have discovered methods that allow any Web site to discover a user's browser history. These methods include the use of Cascading Style Sheets (CSS)

[3] *FTC v. Enternet Media,* No. CV 05-7777 CAS (C.D. Cal., filed Nov. 1, 2005), http://www.ftc.gov/os/caselist/0523135/051110amndcomp0523135.pdf, at 14-15.

or JavaScript to query whether particular sites appear in the history file.[4] As a user browses the Web, any marketer or advertising network could use this technique to read the user's entire browser history, and target ads (or do anything else) based on this information.

In this scenario, the harm to the user's computer (or wallet) may not be immediately evident. But CDT believes – and we think the FTC would agree – that no marketer should be allowed to read a user's entire browser history with no notice and without the user's consent just because he or she chose to visit a site where that marketer was displaying an advertisement. Yet there is currently no policy framework that punishes marketers for doing this.

This scenario exemplifies the gray area encompassed by behavioral advertising. Although the underlying goal may be similar to that of many spyware programs – to track a user's Internet activity and somehow profit from this information – consumers are only weakly protected, if at all, from the privacy impact of behavioral advertising. This concept is explored further in each of the following sections.

Principle I:
A consumer's computer belongs to him or her, not the software distributor. Internet businesses are not free to help themselves to the resources of a consumer's computer.

The first principle speaks to the intuitive notion that software makers should not be able to gain access to or use the resources of a consumer's computer without the consumer's consent. The fundamental idea is that users should be in control of both what comes onto their computers and what can be read from them.

Overriding User Choices

The FTC's most recently completed spyware investigation, involving the Media Motor scam, provides a useful example for applying this principle to behavioral advertising. The defendants in the case were hiding the Media Motor software application within seemingly benign files, such as Internet videos. Consumers who viewed these videos would unwittingly download the Media Motor application, which would then engage in a variety of invasive behaviors, including tracking users' Internet activity. All of this was taking place unbeknownst to the consumer.

[4] See, e.g., *Timing Attacks on Web Privacy (Paper and Specific Issue)*, SecuriTeam, Feb. 20, 2002, http://www.securiteam.com/securityreviews/5GP020A6LG.html; *CSS History Hack Without JavaScript*, http://ha.ckers.org/weird/CSS-history.cgi; *CSS History Hack*, http://ha.ckers.org/weird/CSS-history-hack.html; Jakobsson and Stamm, *Invasive Browser Sniffing and Countermeasures*, Proceedings of the 15th international conference on World Wide Web, 2006, http://www.cs.indiana.edu/~sstamm/papers/invasivesniff05.pdf, at 1-2; Jakobsson et al, *Phishing for Clues*, https://www.indiana.edu/~phishing/browser-recon/.

In the context of behavioral advertising on the Web, one can imagine something of a similar scenario. A user visits a particular Web site, perhaps to view a video or find some other content. If the site includes targeted advertising, the user may receive a cookie containing a unique identifier so that his or her Internet activity can be tracked upon returning to the site or when visiting other sites.

Of course, there is a simple and somewhat well-known way for users to regain control over this logging of their Internet activity – they can delete their cookies. In this scenario, perhaps the user deletes all cookies at the end of the browser session, or runs an anti-spyware program that deletes tracking cookies. This may appear to give control back to users over what is stored on their computers and how they can be tracked.

However, technologies developed within the last several years can provide marketers and advertising networks with a way to work around cookie deletion. In 2005, a company called United Virtualities announced the development of a browser-based Persistent Identification Element (PIE) that can help to restore a deleted cookie, with its original unique identifier, to a user's browser.[5] PIE makes use of "Flash cookies" (also known as local shared objects), which provide storage for the persistent identifier on the user's computer. This storage is available to any Adobe Flash animation embedded within a Web page, which means that this type of technique could be used by marketers and advertising networks even if they are not using United Virtualities' PIE.

Using this kind of technology to override a consumer's decision to remove cookies wrests control from consumers and puts it back in the hands of marketers and advertising networks. In the Media Motor case, and nearly all of the FTC's other spyware enforcement actions, taking control of the computer away from the consumer was considered unfair or deceptive. Of course, all of those cases involved invasive software programs that arguably wreaked greater havoc on consumers' computers than any behavioral advertising currently does. But if the FTC truly believes that "a consumer's computer belongs to him or her," then marketers and advertising networks should not be allowed to override a consumer's choice to remove a cookie file that is used for tracking.

Although deleting cookies may be the most accessible way for consumers to handle the scenario described above, there is, of course, another mechanism – the Network Advertising Initiative (NAI) opt-out, which places an opt-out cookie on the machine of a user who wants to avoid behavioral advertising. As discussed in the next section, however, the NAI opt-out may be very difficult for consumers to find and use. In addition, only a fraction of online advertising networks are NAI members, which means that cookie deletion may still be necessary for users who want comprehensive control over who may use their computers for the purposes of tracking their Internet activity.[6]

---

[5] *United Virtualities Develops ID Backup to Cookies*, Mar. 31, 2005, http://www.unitedvirtualities.com/UV-Pressrelease03-31-05.htm.

[6] Over a two-week period in May 2006, CDT collected advertisements displayed by two deceptively installed adware programs. Over the course of the study, CDT identified 73 advertising intermediaries (advertising networks, affiliate networks, and ad-serving platforms) involved in the delivery of the ads. Only four were members of the NAI, although they all have access to user behavioral data. See *Following*

Under these circumstances, overriding a consumer's choice to delete cookies presents a real threat to user control.

Going Beyond Cookies

Cookies are useful for behavioral advertising purposes because they store data on a user's computer that can later be retrieved by marketers and advertising networks. But cookies are by no means the only mechanism that can be used to store data on users' computers to facilitate tracking of their Internet activities.[7] Other storage mechanisms include:

- **Flash cookies**, as described above, provide a way for Adobe Flash animations embedded within Web pages to store and retrieve information on a user's computer, separate from traditional cookie files.[8]

- **Browser caches** store recently viewed Web content on users' computers for the purposes of speeding up Web browsing. Over the past few years, researchers have demonstrated several different ways that cached content may be exploited to learn about which sites a user has visited or to make inquiries about a user's activity on particular sites.[9]

- **Browser histories** are lists of sites that users recently visited, maintained for the purpose of displaying those sites to the user later on. In a similar fashion to browser caches, history files can be probed to find out where a user has been on the Web.[10]

- **Bookmarks** allow users to maintain lists of their favorite or most frequently visited sites. When a user visits a Web site, some browsers allow the site to detect the user's bookmarks.[11]

---

the Money II: The Role of Intermediaries, Center for Democracy & Technology, Aug. 2006, http://www.cdt.org/privacy/20060809adware.pdf.

[7] These comments only discuss technologies that store data on users' computers, but there are several other techniques that can be used for behavioral advertising that do not rely on such storage. For example, some Internet service providers are providing *complete logs* of their customers' Internet activity to behavioral advertising firms, who then work with marketers to deliver targeted advertisements to those customers. See, e.g., Chris Morrison, *NebuAd offers "deep" targeted advertising, raises nearly $20.5M*, VentureBeat, Sept. 25, 2007, http://venturebeat.com/2007/09/25/nebuad-promises-best-possible-targeted-advertising-at-risk-of-privacy. This is a much more invasive process than anything described in these comments, and companies engaged in these kinds of practices warrant greater scrutiny than they have received to date.

[8] For more information on Flash cookies, see *Local Shared Objects -- "Flash Cookies"*, Electronic Privacy Information Center, Jul. 21, 2005, http://www.epic.org/privacy/cookies/flash.html.

[9] See Jackson et al, *Protecting Browser State from Web Privacy Attacks*, Proceedings of the 15th International Conference on World Wide Web, May 2006, http://crypto.stanford.edu/sameorigin/sameorigin.pdf; *supra* note 4.

[10] *Id.*

[11] See Jakobsson and Stamm, *Invasive Browser Sniffing and Countermeasures*, Proceedings of the 15th international conference on World Wide Web, 2006, http://www.cs.indiana.edu/~sstamm/papers/invasivesniff05.pdf, at 1.

For some of these mechanisms, controls exist that allow users to manage the information that gets stored on their computers and who is allowed to read it, but they are even less straightforward than the traditional cookie deletion process. With Flash cookies, for example, users who want to deny any site from setting a Flash cookie must first somehow find a link to the Adobe Flash Web Storage Settings Panel Web site.[12] Once on the site, users must then turn two different dials (which measure how much storage Flash cookies can use) down to zero kilobytes.[13] Protecting the browser cache, history, or bookmarks requires either installing a special browser plug-in or foregoing the benefits of these features (constantly clearing the browser cache, for example, eliminates the benefit that the cache provides in speeding up the browsing experience).[14]

As with the example described in the previous section, although the NAI opt-out may provide an additional control over these mechanisms, it is neither comprehensive nor simple to use. For consumers to truly be in command of how their computers are used, they need a better way to control how data is stored on their machines and who may read it for the purposes of tracking their Internet activity.

Principle II:
Buried disclosures do not work.

The second principle highlights the fact that burying critical information within a lengthy disclosure document does not provide users with adequate notice. In pursuing its spyware enforcement actions, the FTC has often found that the existence of spyware and other bundled software is only disclosed within a long End User License Agreement (EULA) that users fail to read. In some cases, such as those involving Advertising.com and Odysseus Marketing, this deception ultimately allowed users' Internet activity to be tracked without their prior knowledge.[15]

In the realm of behavioral advertising, the NAI outlines a notice standard for its members to follow. To find information about how an NAI member is tracking a user's Internet activity across multiple Web sites (and how he or she may opt out of such tracking), the process the user must go through might resemble the following:

---

[12] *Flash Player Help: Website Storage Settings Panel*, Adobe, http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html.
[13] These dials can be found at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html and http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html.
[14] Such plug-ins include SafeCache (http://www.safecache.com/) and SafeHistory (http://www.safehistory.com/).
[15] *In the Matter of Advertising.com*, FTC Docket No. C-4186 (filed Aug. 3, 2005), http://www.ftc.gov/os/caselist/0423196/050803comp0423196.pdf at 2; *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005), http://www.ftc.gov/os/caselist/0423205/050929comp0423205.pdf at 6.

1. The user visits a Web site that uses third-party behavioral advertising. Tracking of the user's Internet activity likely begins without the user's knowledge.

2. If the user is aware of the behavioral advertising and wants to learn more about it, he or she must scroll through the site to find its privacy policy.

3. If the site's privacy policy is layered, the user may have to click through several pages to find the section that describes how the site uses behavioral advertising.

4. When the user finds the section on behavioral advertising, it may include a link to NAI information, or it may include separate links to the privacy policies of each of the advertising networks that the site uses. On some sites, this list includes dozens of links.[16]

5. Depending on what links are provided in the site privacy policy, the user must either visit the NAI site or visit each of the individual advertising networks' privacy policies to find information about how they track user Internet activity and how users may opt out.

It is difficult to imagine a more cumbersome process for users. Even in spyware cases where users were presented with an *on-screen* EULA, the FTC felt that the disclosures were sufficiently hidden to be considered deceptive. In the case of behavioral advertising, users are presented with nothing on the screen before the tracking of their activity begins. They must search for the notice, and in some cases they must wade through policy after policy in order to find the information they are looking for. Furthermore, this process only applies to NAI members. For other marketers and advertising networks, there is no standard process for disclosing critical details about how they engage in behavioral advertising.

If buried disclosures are a problem for spyware, they are certainly a problem for behavioral advertising.

Principle III:
If a distributor puts a program on a consumer's computer that the consumer does not want, the consumer should be able to uninstall or disable it.

Many of the FTC's spyware enforcement actions have dealt with software distributors that failed to provide a functioning mechanism for users to remove their software. The analogous issue with behavioral advertising is the failure to provide a robust means for users to avoid having their Internet activity tracked by marketers and advertising networks.

[16] The Terms of Service for the USA Today Web site, for example, list 33 links to third-party advertisers and ad servers that the site uses. See *Terms of Service*, USA Today, Jul. 12, 2005, http://www.usatoday.com/marketing/advertiser-list.htm.

The goal of the NAI opt-out mechanism was to provide this robust way for users to decline behavioral tracking on the Web. As discussed in the previous section, many users may have trouble even finding the opt-out (just as they have difficulty uninstalling software that does not appear on the "Add/Remove Programs" list).

Moreover, the NAI opt-out mechanism, which places an opt-out cookie on a user's computer, simply cannot be considered robust. Cookies are too easily deleted and corrupted. Users may remove their own opt-out cookies by mistake, or anti-spyware programs may delete them.

In the FTC's spyware complaint against Sony BMG, the Commission faulted the company because its uninstall process required more than "reasonable efforts" on the part of the consumer.[17] Asking the user to go through the process outlined in the previous section every time the opt-out cookie is deleted can hardly be considered reasonable. If the FTC uncovered a software uninstall process working this way – where every time the user deleted the "uninstall" file, the software would reappear – it would undeniably be considered an unfair or deceptive practice.

Aside from the NAI opt-out mechanism, users can attempt to manage the tracking of their Internet activity on their own. But as described in the discussion of the first principle, this can be extremely complicated. Marketers and advertising networks may also be able to find ways to work around a user's opt-out, much as software developers – like those involved in the Movieland and DirectRevenue cases – have found ways to work around a user's uninstall choice.[18]

Conclusion

The three FTC spyware principles serve as a useful starting point for developing a policy prescription for behavioral advertising, but they do not provide a complete framework. CDT is hopeful that by conceptualizing behavioral advertising in light of work that the FTC has already done, comprehensive privacy protections can be applied to one of the practices that underlies both spyware and behavioral advertising – the tracking of users' Internet activity without proper user control. The FTC has already laid the groundwork to bring our inadequate policies for protecting privacy in behavioral advertising up to the level that consumers deserve. CDT looks forward to exploring this idea further at the Town Hall and beyond.

---

[17] *In the Matter of Sony BMG Music Entertainment*, FTC Docket No. C-4194 (filed Jan. 30, 2007), http://www.ftc.gov/os/caselist/0623019/0623019cmp070629.pdf at 4.

[18] *FTC v. Digital Enterprises, Inc., et* al, No. CV06-4923 (C.D. Cal., filed Aug. 8, 2006), http://www.ftc.gov/os/caselist/0623008/060808movielandcmplt.pdf at 17-18; In *the Matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook*, FTC File No. 052 3131 (filed Feb. 16, 2007), http://ftc.gov/os/caselist/0523131/index.htm at 5.