NOTE

A PATH TOWARD USER CONTROL OF ONLINE PROFILING

Tracy A. Steindel[*]

Cite as: Tracy A. Steindel, *A Path Toward User Control of Online Profiling*, 17 MICH. TELECOMM. TECH. L. REV. 459 (2010), *available at* http://www.mttlr.org/volseventeen/steindel.pdf

INTRODUCTION

Online profiling is "the practice of tracking information about consumers' interests by monitoring their movements online."[1] A primary purpose of online profiling is to "deliver advertising tailored to the individual's interests," a practice known as online behavioral advertising (OBA).[2] In order to accomplish this, publishers and advertisers track an

* J.D., University of Michigan Law School, 2011; Executive Note Editor, *Michigan Telecommunications and Technology Law Review*. I am grateful to Professor Jessica Litman for her insightful comments and to *MTTLR*'s editors, particularly Liz Allen.

1. *Glossary of Interactive Advertising Terms v. 2.0*, INTERACTIVE ADVERTISING BUREAU, 20 (Oct. 17, 2001), http://www.iab.net/media/file/GlossaryofInteractivAdvertisingTerms.pdf.

2. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 1 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter 2009 REPORT]. The Federal Trade Commission includes tracking within its

individual's online behavior using cookies and other means. Publishers and advertisers aggregate the information, often compile it with information from offline sources, and sort individuals into groups based on characteristics such as age, income, and hobbies. Advertisers can then purchase access to these consumer groups, controlling their selections with such specificity that one commentator has compared the process of choosing the most desirable targets to "fishing from a barrel."[3]

The online advertising industry has maintained that, far from being a cause for concern, OBA and, by extension, online profiling are helpful to consumers and provide significant economic benefits to publishers, the advertising industry, and consumers. Consumer privacy advocates, among others, argue that online profiling is an invasion of privacy, does not accord with users' expectations, and even invites discriminatory practices.

The benefits and dangers of online profiling continue to be disputed, even as online profiling remains largely unregulated. Congress has not passed any relevant legislation, and courts have proven unwilling to read existing legislation to prohibit or limit online profiling.[4] The Federal Trade Commission (FTC) has made some efforts to address online profiling, relying upon its authority over unfair and deceptive trade practices.[5] Although the FTC has promoted and guided industry self-regulation regarding OBA,[6] it has recognized the need for "legislation that would set forth a basic level for privacy protection for all visitors to consumer-oriented commercial Web sites with respect to profiling."[7] The FTC is not alone in this view: at least two draft bills were presented to

---

definition of OBA. This blurs the line between online profiling and OBA, which extends the less pejorative term—behavioral advertising—to the practice of tracking users. *See* Brian Stallworth, Note, *Future Imperfect: Googling for Principles in Online Behavioral Advertising*, 62 FED. COMM. L.J. 465, 478 (2010). This Note will use "online profiling" to refer to the process of tracking individuals and "OBA" to refer to the delivery of targeted advertisements.

3. ROB GRAHAM, FISHING FROM A BARREL: USING BEHAVIOR TARGETING TO REACH THE RIGHT PEOPLE WITH THE RIGHT ADS AT THE RIGHT TIME 16 (2006), *available at* http://online-behavior.com/wp-content/uploads/Fishing-From-a-Barrel.pdf.

4. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (holding that an Internet advertising corporation's use of cookies to track users did not violate the Electronic Communications Privacy Act, the Federal Wiretap Act, or the Computer Fraud and Abuse Act).

5. 15 U.S.C. § 45(a) (2006); *see also* FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 17 (2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter 2000 REPORT] ("The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ('FTCA'), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. . . . Commerce on the Internet falls within the scope of this statutory mandate.").

6. 2009 REPORT, *supra* note 2, at 481.

7. FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS, PART 2 RECOMMENDATIONS 10 (2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf [hereinafter 2000 REPORT PART 2].

the 111th Congress;[8] the New York Assembly is debating a proposal;[9] and the Department of Commerce's Internet Policy Task Force has called for the creation of a Privacy Policy Office.[10]

Part I of this Note presents an overview of the technologies that enable online profiling and the ways in which the online advertising industry uses gathered information to target users. Part II argues that legislation regulating online profiling is necessary because profiling is a harmful practice that users cannot prevent and for which no remedy is available. Part III examines the FTC's recent proposal for a 'do not track' mechanism and proposes elements that future legislation should include in order to allow this mechanism to effectively address some of the concerns online profiling raises.

I. WHAT IS ONLINE PROFILING?

A. *Technology*

Advertisers and publishers employ a variety of technologies to amass records of users' online activities. Broadly speaking, these technologies enable an ongoing string of communication between a user's computer and a website or an advertiser, allowing the website or advertiser to follow the user within and between websites. This subsection will provide a brief explanation of the ways in which two common mechanisms—cookies and web beacons—and one developing mechanism—HTML5—track individual behavior.

Cookies are small text files that store information on computers' hard drives; web servers place them on hard drives and use them to retrieve the information they store. Cookies can contain unique identification numbers, which allow servers to recognize and remember users. They have many legitimate uses, such as storing users' preferences, passwords, and items in online shopping carts. They also allow websites to track the activities of users within the site in order to improve the site or to suggest products based on users' browsing histories.[11]

Cookies are site-specific, but they can still be used to track users' behavior across multiple sites. In addition to its own cookies, a website

8. Best Practices Act, H.R. 5777, 111th Cong. (2010); Boucher/Stearns Discussion Draft, 111th Cong. (2010) (on file with author).

9. Online Consumer Protection Act, Gen. Assemb. B. A4809, 2011 Leg., 234th Reg. Sess. (N.Y. 2011).

10. DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 44–50 (2010), *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

11. Marshall Brain, *How Internet Cookies Work*, HOWSTUFFWORKS, http://computer.howstuffworks.com/cookie.htm (last visted Mar. 8, 2011).

might allow a third party to place a cookie on a user's hard drive. For example, the ad network DoubleClick might place a cookie on a user's computer when the user visits a website that displays ads supplied by DoubleClick. If the user then visits an unrelated site on which DoubleClick also advertises, DoubleClick will recognize the cookie it previously deposited and be able to track the user's activities on both sites. This tracking can continue across as many websites as an advertiser has cookies, allowing an advertiser to build a detailed profile of a user's online activity.[12]

Users can delete standard cookies using a browser's controls. However, at least two permutations—the Flash cookie and the Evercookie—evade simple deletion. Adobe's Flash software allows websites to store up to twenty-five times the amount of information of a regular cookie. This permits large sound and video files to pre-load enough information to ensure smooth playback. The software can also store data from cookies, recreating cookies with the same unique identification number even after a user deletes the originals.[13] As a result, Flash cookies are difficult to remove permanently. "Erasing HTTP cookies, clearing history, erasing the cache, or choosing a delete private data option" are all ineffective, as is the use of a "Private Browsing" setting.[14] Users can control their Flash player privacy settings through the Settings Manager, but the interface is so confusing that Adobe fears users will mistake the actual Settings Manager for a static, instructional image.[15] The Evercookie is even more persistent than Flash cookies. It stores cookie data in up to thirteen locations; when a user deletes information from one location, the remaining locations recreate it.[16] Needless to say, this makes it difficult for users to find and delete all copies before the remaining copies regenerate them.[17]

12. *Id.*

13. Ashkan Soltani et al., Flash Cookies and Privacy 3 (Aug. 10, 2009) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 ("We found that taking the privacy-conscious step of deleting HTTP cookies to prevent unique tracking could be circumvented through 'respawning' . . . . The flash cookie value would be rewritten in the standard HTTP cookie value, thus subverting the user's attempt to prevent tracking.").

14. *Id.* at 1.

15. *Flash Player: Settings Manager—Global Privacy Settings Panel*, ADOBE, http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html#118539 (last visited Mar. 8, 2011) ("Note: The Settings Manager that you see above is not an image; it is the actual Settings Manager. Click the tabs to see different panels . . . .").

16. Samy Kamkar, *Evercookie—Never Forget*, SAMY.PL (Sept. 20, 2010), http://samy.pl/evercookie/.

17. Jacqui Cheng, *Zombie Cookie Wars: Evil Tracking API Meant to "Raise Awareness,"* ARS TECHNICA, http://arstechnica.com/web/news/2010/09/evercookie-escalates-the-zombie-cookie-war-by-raising-awareness.ars (last visited Apr. 11, 2011) (referring to the process of deleting Flash cookies as "a daunting task even for the relatively experienced surfer").

For all their variety, cookies are just one of many mechanisms that track users. Web beacons are another. Unlike cookies, which are stored on users' computers, web beacons are embedded in web pages' HTML codes, typically as small graphics. Whenever a user accesses a website, the browser transmits information to the website's servers; this information typically includes the IP address of a user's computer, the URL requested, the type of browser, and so on. Third parties who have placed web beacons on a website can also view this information.[18] Web beacons can even communicate with third-party cookies, allowing the tracker to identify the individual user if the IP address alone did not already allow it to do so.[19]

HTML5 enables new developments in user tracking practices.[20] HTML5 is the fifth iteration of the Hyper Text Markup Language, the code used to create web pages. It is able to collect and store large amounts of data on users' hard drives. This has many advantages; for instance, it will make it possible to access multimedia content without relying on third-party software such as Adobe's Flash player, and it will allow users to check e-mail offline.[21] However, the greater quantity of information stored on users' hard drives will permit trackers to acquire even more information about them. Furthermore, some devices, including the iPhone and iPad, do not allow users to clear the browser databases stored on their devices, making it impossible to avoid tracking.[22] Faced with these capabilities, Pam Dixon, the executive director of the World Privacy Forum, has warned, "HTML5 opens Pandora's box of tracking in the Internet."[23]

18. *Web Beacons and Other Tools*, ALL ABOUT COOKIES, http://www.allaboutcookies.org/web-beacons/index.html (last visited Mar. 8, 2011).

19. Joshua Gomez et al., *KnowPrivacy*, KNOWPRIVACY, 8–9 (June 1, 2009), http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

20. This new standard has not yet been ratified, although some sites are already employing it. Mikal E. Belicove, *Understanding HTML5 and Why It Matters*, ENTREPRENEUR.COM DAILY DOSE (Feb. 4, 2010), http://blog.entrepreneur.com/2010/02/understanding-html5-and-why-it-matters.php.

21. *See, e.g.*, Tanzina Vega, *New Webcode Draws Concern Over Privacy Risks*, N.Y. TIMES, Oct. 10, 2010, at A1, *available at* http://www.nytimes.com/2010/10/11/business/media/11privacy.html?pagewanted=1&_r=1&hp; Iljitsch van Beijnum, *Safari Team: "Webkit Does HTML5 Client-side Database Storage,"* ARS TECHNICA, http://arstechnica.com/apple/news/2007/10/safari-team-webkit-does-html5-client-side-database-storage.ars (last visited Apr. 11, 2011).

22. Jacqui Cheng, *Advertisers Get Hands Stuck in HTML5 Database Cookie Jar*, ARS TECHNICA, http://arstechnica.com/apple/news/2010/09/rldguid-tracking-cookies-in-safari-database-form.ars (last visited Apr. 11, 2011).

23. Vega, *New Webcode*, *supra* note 21.

Cookies, web beacons, and HTML5 are by no means the only tracking mechanisms that exist.[24] Nonetheless, they do provide a snapshot of the advantages and potential pitfalls of common tracking technologies. While, they enable many of the features on which online sites rely, including shopping carts and the ability to view videos, they also enable user tracking and can evade deletion through a variety of regenerative tactics.

B. *Industry*

"The essence of the advertising industry is to solve a massive matching problem: a large number of advertisers want to deliver multiple messages to a large number of consumers."[25] OBA, which is only one form of online advertising, allows advertisers to make more efficient decisions regarding which users are likely to respond to which advertisements. The premise of OBA is fairly simple. The more an advertiser watches a consumer, the more likely it is to learn about him; the more an advertiser learns about a consumer, the more accurately the advertiser can suggest an offer that meets the consumer's needs.[26] Recent studies have upheld this theory. One found that OBA improves click-through rates by 670% over "run of network advertising,"[27] and another study sponsored by the Network Advertising Initiative found that the percentage of clicks from OBA that resulted in sales was more than twice that of run of network advertising.[28] Graham compares run of network advertising to "passing fliers out on a busy street corner,"[29] whereas OBA presents advertisers with the opportunity "to start real conversations with consumers who represent real customers and not just random passersby."[30]

---

24. *See, e.g.*, Andrew N. Person, *Behavioral Advertising Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience*, 62 FED. COMM. L.J. 435, 439 (2010) ("Currently, DPI provides information about the online tendencies of Internet users by reviewing search engine queries, recognizing trends with the frequency of consumer Web site visits, and recording the types of applications that consumers are using online.").

25. David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, J. ECON. PERSP., Summer 2009, at 37, 43.

26. GRAHAM, *supra* note 3, at 16.

27. HOWARD BEALES, THE VALUE OF BEHAVIORAL TARGETING 11 n.9 (2010) (citing JUN YAN ET AL., HOW MUCH CAN BEHAVIORAL TARGETING HELP ONLINE ADVERTISING? (2009)), *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. "Run of network advertising" refers to the placement of an ad by an ad network across its entire network. *Id.* at 20. Thus, all users visiting all sites from whom the advertiser purchases space will see the same ad.

28. *Id.* at 12.

29. GRAHAM, *supra* note 3, at 79.

30. *Id.* at 5.

How does this all work? The FTC explains, "Consumer data can be analyzed and combined with 'psychographic' data from third-party sources, data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms. This enhanced data allows the advertising networks to make a variety of inferences about each consumer's interests and preferences."[31] For example, a user might search for flights to New York on a travel site, at which time an advertiser installs a cookie. The user then visits the website of a local newspaper, which is part of the same advertising network, to read about a local sports team. The advertiser at the news site recognizes its cookie, sees that the user has an interest in both travel to New York and sports, and displays an ad referring to the New York Yankees.[32]

A variety of different parties may participate in collecting, aggregating, and disseminating information about users and using that information to buy and sell ad space. The FTC's pictorial representation of the "personal data ecosystem" shows that retail and content sites, social networking sites, and search engines all track users.[33] They sell or share the information with affiliates, information brokers, web sites, catalog co-ops, and ad network and analytic companies; these parties, in turn, sell or share the information with banks, employers, marketers, the media, the government, law enforcement, lawyers and private investigators, individuals, and product and service delivery companies.

Of these many parties, publishers, ad networks, and analytics companies are the most involved in OBA. Howard Beales, former Director of the Bureau of Consumer Protection at the FTC, explains,

> Large publishers with diverse content offerings can use behavioral targeting across their various sites to offer their users more targeted ads. Additionally, third party firms can specialize in parts of this process or can encompass all of it, offering targeting across a broad range of publisher content. For example, data exchanges specialize in data collection and analytics that they sell to advertisers. More comprehensive third party advertising networks . . . can handle both the collection, analytics, and servicing of the ads.[34]

31. 2000 REPORT, *supra* note 5, at 5.

32. 2009 REPORT, *supra* note 2, at 3–4.

33. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS app. C (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter 2010 REPORT].

34. BEALES, *supra* note 27, at 12.

DoubleClick is a well-known example of a third-party advertising network. Many websites wish to rent online "space" to advertisers in which advertisers may display ads, such as the banners commonly seen at the top of a webpage. DoubleClick acts as an intermediary between websites and advertisers, promising advertisers that it will display their ads on webpages to users who match the desired demographic.[35]

Websites sell their advertising space though a bidding process. For example, an advertiser may inform a third-party advertising network that the advertiser will pay a given amount to display ads to users with certain characteristics. When such a user visits a website, the ad network submits the advertiser's bid, and the highest bidder wins the ability to display their ad to that user.[36] The largest ad exchanges place billions of ads each day,[37] and the development of real-time bidding (RTB) allows advertisers to target users with ever-increasing specificity. Previously, advertisers had to predict in advance who was likely to visit a page and place their bids accordingly. RTB allows advertisers to bid to serve ads in the milliseconds it takes for a page to load, providing advertisers with an opportunity to evaluate their bid based on the specific user requesting the page.[38]

II. THE NEED FOR REGULATION

A. *Online Profiling Is a Harmful Practice*

The average person expects some control over information relating to him or her. This is evident in the strong public outcries against changes in the privacy policies of common sites, such as Facebook and Google. For instance, Google suffered widespread condemnation when it introduced Google Buzz, because Buzz automatically published lists of followers based on the people a user contacted the most.[39] Google ulti-

35. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001).

36. Christian Borgs et al., Dynamics of Bid Optimization in Online Advertisement Auctions 1–2 (2007) (unpublished manuscript), *available at* http://www2007.org/papers/paper089.pdf (providing a discussion of the bidding process for search-based advertising).

37. Complaint at 2, Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy (filed F.T.C. Apr. 8, 2010) (Complaint, Request for Investigation, Injunction, and Other Relief) (stating that "Yahoo's Right Media Exchange processes 9 billion transactions daily" and "MediaMath serves more than '13 billion impressions a day'").

38. Stephanie Clifford, *Instant Ads Set the Pace on the Web*, N.Y. TIMES, Mar. 11, 2010, at B1, *available at* http://www.nytimes.com/2010/03/12/business/media/12adco.html?_r=1.

39. *See, e.g.*, Nicholas Carlson, *Warning: Google Buzz Has a Huge Privacy Flaw*, BUS. INSIDER (Feb. 10, 2010, 4:49 PM), http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2; Evgeny Morozov, *Wrong Kind of Buzz Around Google Buzz*, NET EFFECT (Feb. 11, 2010, 6:20 AM), http://neteffect.foreignpolicy.com/posts/2010/02/11/wrong_

mately faced a class action lawsuit, which it has preliminarily agreed to settle for $8.5 million.[40] Meanwhile, even those users who do not appear incensed over Facebook's regular privacy-related gaffes[41] fill Facebook's blogs with requests for greater control over the information they share.[42]

The expectation of control over personal information is also evident in a number of traditional conceptions of privacy. Daniel Solove, a professor at the George Washington University Law School, summarized three concepts that are particularly relevant to the control of information.[43] The first is a right of "limited access to the self." As explained by an early theorist, E.L. Godkin, this includes "the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion."[44] Second, and closely associated with the concept of limited access, is the constitutionally recognized expectation that confidential information will remain so, what Solove terms "secrecy."[45] A third approach believes that the core of privacy is the ability to control when and with whom a party shares his personal information.[46] Common to all of these theories is the idea that people should retain some measure of control over information related to them.

People's expectation that they can control such information extends to online activities. One study found that sixty-two percent of Americans believe that websites with privacy policies cannot share information

---

kind_of_buzz_around_google_buzz; Robin Wauters, *Google Buzz Privacy Issues Have Real Life Implications*, TECHCRUNCH (Feb. 12, 2010), http://techcrunch.com/2010/02/12/google-buzz-privacy.

40. *Overview of the Proposed Settlement*, GOOGLE BUZZ USER PRIVACY LITIGATION, http://www.buzzclassaction.com (last visited Mar. 27, 2010).

41. *See Facebook Privacy*, EPIC.ORG, http://epic.org/privacy/facebook/ (last visited Mar. 27, 2011) (providing an extensive compilation of news regarding Facebook).

42. *See, e.g.*, Nadia M. DeMartino, Comment to *Improving Transparency Around Privacy*, THE FACEBOOK BLOG (Dec. 23, 2010, 8:10 AM), http://blog.facebook.com/blog.php?post=167389372130 ("I don't enjoy how everyone can see every little thing I write on someone's wall."); Jared Drew, Comment to *Updates on Your New Privacy Tools*, THE FACEBOOK BLOG (June 2, 2010, 4:55 PM), http://blog.facebook.com/blog.php?post=197943902130 ("I don't want them to know who's [sic] friends we share mutually."); Roberta A. Morad, Comment to *New Tools to Control Your Experience*, THE FACEBOOK BLOG (Oct. 18, 2010, 1:06 AM), http://blog.facebook.com/blog.php?post=196629387130 ("WE [sic] the FB Members need to decide whether we want our phone contacts and email addresses to be public from Yahoo or MSN etc.").

43. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099–124 (2002). Solove ultimately argues that each of these conceptualizations, even the very act of creating an overarching conception of privacy, is inherently over- or under-inclusive. *Id.* at 1125–26. Nonetheless, the categories present a useful summary of accepted concepts of privacy.

44. *Id.* at 1103.

45. *Id.* at 1106 (citing Whalen v. Roe, 429 U.S. 589 (1977)).

46. *Id.* at 1109–10.

about users with other companies without first obtaining users' permission, and when asked if companies must have permission to follow users across multiple sites, the majority of respondents believed that this was true or did not know.[47] This widespread, erroneous understanding of tracking and online profiling practices indicates that these practices are contrary to users' intuitive privacy expectations.

Once users are aware of online profiling, their reactions to the practice range from simple concern to feelings of violation, again demonstrating an expectation that the practice should not be the norm. One survey found that seventy-two percent of consumers are "concerned" that their activities are tracked online, and ninety-three percent believe companies should not use personal information without permission.[48] Another survey shows that sixty-six percent of American respondents do not want to receive tailored advertising, and eighty-four percent reject tailored advertising that involves tracking their behavior between websites.[49] After receiving OBA for the first time, one advertising executive even admitted, "Intellectually I have totally accepted behavioral targeting and even welcome it as an advertiser, but emotionally and as a prospect, I'm still not sure. I had no idea I would be so prudish about this until it actually happened. . . . I do feel a little violated."[50]

Online profiling is a harmful practice precisely because it is contrary to traditional concepts of privacy and user expectations, which both reflect the belief that privacy includes some measure of control over personal information. Just as a "Peeping Tom" offends by viewing victims in places in which the victims expect to be out of the public view, publishers and advertisers harm users by following their activities through areas in which the users—rightly or wrongly—believe themselves to be unobserved.

Although the violation of user expectations may fall outside of legally cognizable privacy-related harms, the FTC argues that "the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private

47. Joseph Turow et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It*, SSRN, 21 (Sept. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

48. *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMERSUNION.ORG (Sept. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

49. Turow et al., *supra* note 47, at 14.

50. Gord Hotchkiss, *Hello, My Name Is Gord, and I've Been Behaviorally Targeted*, SEARCH INSIDER (Apr. 12, 2007, 9:30 AM), http://www.mediapost.com/publications/index.cfm?fuseaction=Articles.showArticle&art_aid=58602.

information 'out there.'"[51] The FTC's new approach to conceptualizing the harms of online profiling fits within other calls for a more flexible approach to privacy. Solove, for instance, argues that "not all privacy problems are the same, and different conceptions of privacy work best in different contexts. Instead of trying to fit new problems into old conceptions, we should seek to understand the special circumstances of a particular problem."[52] Under the FTC's new approach, online profiling is harmful precisely because it occurs despite user's expectations and wishes to the contrary.

Online profiling is harmful not only because it is contrary to expectations, but also because it limits the options available to users. Martin Abrams has termed this "boxing." Boxing occurs when "a consumer's vision and choices are limited by his or her digital history and the analytics that make judgments based on that digital history."[53] This may take the form of variable pricing, a practice in which retailers review a user's past searching and buying history and adjust their prices to reflect the user's perceived willingness to pay more.[54] Beyond mere pricing, online profiling may affect options presented to consumers regarding major financial decisions. For example, Capital One admits that it uses browsing history to suggest different credit cards to different individuals,[55] and the Center for Digital Democracy presents the possibility that sub-prime mortgage lenders might have used online profiling to target low-income black and Hispanic Internet users.[56] At least one user claims to have received different loan offers depending on which Internet browser he used.[57] The Fair Credit Reporting Act governs the actual lending practices of these institutions; however, nothing limits their ability to suggest or promote certain offers, and users who are unaware of OBA may not

51. 2010 REPORT, *supra* note 33, at 20.

52. Solove, *supra* note 43, at 1147.

53. Martin Abrams, Guest Headnote, *Boxing and Concepts of Harm*, 4 PRIVACY & DATA SEC. L.J. 673, 673 (2009).

54. Annie Lowrey, *How Much Is That Doggie in the Browser Window?*, SLATE (Dec. 6, 2010, 6:25 PM), http://www.slate.com/id/2276918; *see also* Joseph Turow et al., Open to Exploitation: America's Shoppers Online and Offline 10 (June 1, 2005) (unpublished manuscript), *available at* http://repository.upenn.edu/asc_papers/35/.

55. However, Capital One denies using the information to make lending decisions. Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, at A1, *available at* http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

56. CENTER FOR DIGITAL DEMOCRACY & U.S. PUB. INTEREST RESEARCH GROUP, COMPLAINT AND REQUEST FOR INQUIRY AND INJUNCTIVE RELIEF CONCERNING UNFAIR AND DECEPTIVE ONLINE MARKETING PRACTICES 33–34 (2007), *available at* http://www.centerfordigitaldemocracy.org/sites/default/files/FTCsupplemental_statement1107_0.pdf.

57. CmdrTaco, *Do Firefox Users Pay More for Car Loans?*, SLASHDOT (Nov. 4, 2010, 9:21 AM), http://news.slashdot.org/story/10/11/04/132257/Do-Firefox-Users-Pay-More-For-Car-Loans.

know to actively seek out options other than those advertisers initially suggest based upon the user's profile. Abrams aptly notes the irony that the Internet, a powerful information tool, should become a means of limiting users' options and perspectives, and—just as the FTC calls for setting aside the traditional harms-based approach—Abrams calls for recognition of a new "social" harm: the inability to leave the box.[58]

Even as online profiling determines the very options presented to consumers, there is currently no way to ensure that an individual consumer's compiled profile is accurate. Tracking is tied to computers, not users. If multiple people use the same computer, the resulting profile may not be an accurate reflection of any of them. Confusion can result from just one user's actions: consumers do not research only those matters that relate directly to them. If a user researches eating disorders and spends time on pro-Ana websites[59] in an effort to learn about a friend's eating disorder, will a life insurance company believe that the user suffers from the disease or is at risk of developing an eating disorder?[60] These inaccuracies highlight the dangers of basing discriminatory advertising on information gathered through profiling. The risk of harm extends beyond delivery of OBA; the FTC reports that "some data brokers sell identity verification services to various public and private entities," and inaccurate information can cause such entities to deny benefits to eligible consumers.[61]

Finally, online profiling relies upon the collection of vast quantities of information. One author argues that, as a result of such large databases, "[a]lmost every person in the developed world can be linked to at

58. Abrams, *supra* note 53, at 675.

59. "Pro-Ana" websites promote an anorexic lifestyle. *See, e.g.*, Bonnie Rothman Morris, *A Disturbing Growth Industry: Web Sites That Espouse Anorexia*, N.Y. TIMES, Jun. 23, 2002, § 15, at 8, *available at* http://query.nytimes.com/gst/fullpage.html?res=9F00E4DB123CF930A15755C0A9649C8B63&sec=&spon=&pagewanted=all.

60. Recent research by life insurance companies shows that consumer profiles, based in large part on information gathered from online activity, can be as accurate a predictor of longevity as medical tests. Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J., Nov. 19, 2010, at A1, *available at* http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html?mod=WSJ_article_related. It remains unclear how this use of data would fare under the Fair Credit Reporting Act or insurance regulations, but life insurers might one day use it to determine eligibility for coverage or set premiums. Natasha Singer, *Privacy Groups Fault Online Health Sites for Sharing User Data with Marketers*, N.Y. TIMES, Nov. 23, 2010, at B3, *available at* http://www.nytimes.com/2010/11/24/business/24drug.html?_r=1&scp=1&sq=Privacy%20Groups%20Fault%20Online%20Health%20Sites%20for%20Sharing%20User%20Data%20with%20Marketers&st=cse.

61. 2010 REPORT, *supra* note 33, at 48.

least one fact in a computer database that an adversary could use for blackmail, discrimination, harassment, or financial or identity theft."[62]

B. *Users Cannot Effectively Prevent Online Profiling*

Several studies have demonstrated that consumers are unaware of the extent of tracking that occurs.[63] As an initial matter, if users do not know about online profiling and online tracking, they do not realize they should take what limited protective measures exist. Even those users who do wish to take protective measures have very few options.

Current industry practice relies upon a "notice-and-choice" regime. The notice-and-choice model "encourages companies to develop privacy notices describing their information collection and use practices to consumers, so that they can make informed choices."[64] However, use of a website constitutes consent to its privacy terms. It is almost laughable to think that such a system grants users any real means of preventing unwanted tracking. Most privacy policies are in lengthy legalese; few users are willing—or able—to read and understand them. Indeed, one study shows that the majority of users mistakenly believe that the mere existence of a privacy policy means that websites will not share their information.[65] Assuming a user reads and understands a privacy policy, his or her only means of objecting to its profiling practices is to leave the website; this effectively prevents the use of any website.

The Network Advertising Initiative (NAI), a group of online advertising companies, purportedly eases the burden on consumers by requiring its members to meet certain privacy standards; consumers who visit member sites can presumably trust the websites' privacy practices without needing to review each privacy policy. However, compliance with the NAI is not monitored by an independent third party. The Center for Democracy and Technology argues that this is necessary because most consumers do not have the ability to identify violations,[66] and the self-interested industry cannot be "player, referee, and rule maker."[67]

---

62. Paul Ohm, *Broken Promise of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1748 (2010).

63. Turow et al., *supra* note 47.

64. 2010 REPORT, *supra* note 33, at iii.

65. Turow et al., *supra* note 47, at 21.

66. CENTER FOR DEMOCRACY AND TECHNOLOGY, RESPONSE TO THE 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT FOR ONLINE BEHAVIORAL ADVERTISING 4 (2008), *available at* http://www.cdt.org/privacy/20081216_NAIresponse.pdf.

67. Marvin Ammori, Op-Ed., *Impose Real Privacy Rules*, N.Y. TIMES (Dec. 2, 2010, 3:41 PM), http://www.nytimes.com/roomfordebate/2010/12/02/a-do-not-call-registry-for-the-web/impose-real-privacy-rules.

Thus, membership in the NAI is not an effective indicator of websites' privacy practices.

In addition, there are several "seal" programs that purportedly increase the effectiveness of the notice-and-choice regime. These programs establish certain privacy standards and place their seal on websites meeting those standards. In theory, the seals—or absence thereof—alert users to websites' practices without requiring users to read every privacy policy.[68] Unfortunately, the seal programs do not meet these goals. Seal programs rarely withdraw seals in response to violations; indeed, the program administrators are often unaware of violations. Not only do different programs set different requirements, but individual seal programs do not require uniformity among the sites they certify.[69]

Users may "opt out" of tracking by individual companies, but this is also inadequate. For instance, a user may visit the DoubleClick website and select an option to block tracking by DoubleClick.[70] It would be extremely difficult for a user to individually opt out of all tracking in this way; the user would not only have to visit each site but also figure out which sites to visit in the first place.

Some industry groups do provide a single site at which users may opt out of tracking by some or all members, but this is not an effective solution. First, users must identify the relevant industry groups. Second, the industry chooses the opt-out mechanism available to users. For example, the NAI allows users to replace its members' cookies with "opt-out cookies" specific to each member, preventing the member from using its cookie to track the user.[71] However, whenever users delete their cookies, they also delete the NAI opt-out cookie; some security protection pro-

68. *See, e.g.*, TRUSTE, http://www.truste.com/index.html (last visited Dec. 7, 2010).

69. Ethan Hayward, Note, *The Federal Government As Cookie Inspector: The Consumer Privacy Protection Act of 2000*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y 227, 233–35 (2001). The lack of uniformity between programs means that consumers have to familiarize themselves with with each seal program's requirements.

70. *Advertising and Privacy*, GOOGLE, http://www.google.com/privacy/ads/ (last visited Jan. 16, 2011).

71. *How Does the NAI Opt-out Tool Work?*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/faqs.asp#question_9 (last visited Apr. 10, 2011); *Opt Out of Behavioral Advertising*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/opt_out.asp (last visited Apr. 10, 2011). In addition, the NAI has recently unveiled an "Advertising Option Icon," which is to be displayed near advertisements; users can click on the icon to learn more about the company's data collection and access an opt-out option. Press Release, Network Advertising Initiative, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.networkadvertising.org/pdfs/Associations104release.pdf.

grams even delete opt-out cookies in their normal course of operations.[72] Regardless of the cause, deletion requires the user to opt out all over again.[73] Finally, the membership of an industry group determines the effectiveness of opting out. For example, the NAI simply does not apply to non-members, some of whom have troubling practices,[74] and membership is subject to change without notice.[75]

Users who do attempt to control tracking through the tools individual websites offer face another hurdle: the settings are often so confusing and complex as to be unusable. For examples, one need only look at the Google dashboard,[76] Adobe's Settings Manager,[77] or the Facebook privacy tool.[78]

Some Internet browsers have introduced tools designed to assist users who wish to block tracking; however, these are of limited use. The latest iteration of Microsoft's Internet Explorer browser, IE9, will include a "Tracking Protection List" into which users can enter sites the browser may not "call" unless the user grants permission, but the list is empty by default.[79] To avoid creating a cumbersome opt-in mechanism that will place a large burden on users to identify and enter each individual site they wish to block, IE9 will allow third parties to create lists that users may adopt in their entirety.[80] However, users who wish to block all tracking cannot select that option; they must instead invest substantial resources in personal research or rely on third parties to be thorough and keep their lists updated.

---

72. Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, WORLD PRIVACY FORUM, 17–18 (Nov. 2, 2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

73. Google has recently introduced a plug-in for its browser, Chrome, that will prevent deletion of opt-out cookies. JC Torpey, *'Keep My Opt Out' Chrome Extension Is a Supercharged Google Ad Preferences Manager*, YAHOO! (Jan. 25, 2011, 6:26 PM), http://news.yahoo.com/s/ac/20110125/tc_ac/7702460_keep_my_opt_out_chrome_extension_is_a_supercharged_google_ad_preferences_manager. However, only Chrome's users benefit from this.

74. For instance, RapLeaf is not a member of the NAI. RapLeaf attaches names to the personally identifiable information it collects, and its efforts to strip that information before selling it have not always been thorough. Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., Oct. 25, 2010, at A1, *available at* http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

75. Dixon, *supra* note 72, at 14 ("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.").

76. *Google Dashboard*, GOOGLE, http://www.google.com/dashboard (last visited Dec. 7, 2010).

77. *Flash Player Help*, *supra* note 15.

78. *Facebook Privacy: A Bewildering Tangle of Options*, N.Y. TIMES, May 12, 2010, at B8, *available at* http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html.

79. Dean Hachamovitch, *IE9 and Privacy: Introducing Tracking Protection*, IEBLOG (Dec. 7, 2010 10:10 AM), http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx.

80. *Id.*

Google has also introduced a new feature to its Chrome browser: "keep my opt-outs." This will prevent users from deleting opt-out cookies when they clear their cookies.[81] However, this system still places a burden on users to opt out of cookies in the first place, whether through an incomplete organization, such as the NAI, or through individual companies' websites. Furthermore, it only limits tracking by cookies; it will not reach other tools, such as web bugs or HTML5.

In contrast to IE9 and Google's technology-based solutions, Mozilla has announced an honor system: once a user has enabled the feature, Mozilla will send a constant signal to advertisers, informing them that the user does not wish to be tracked.[82] The most obvious flaw with Mozilla's system is that it expects advertisers to comply with users' wishes. Finally, users may only enjoy these browser features when they use the browser that offers them, and not all devices support these browsers.[83]

Lastly, as discussed above, Flash cookies, Evercookies, and the inability to clear browser databases when using HTML5 make it very difficult for users to delete some undesired tracking mechanisms.[84]

To summarize, users purportedly control online profiling through a notice-and-choice regime under which use of a website constitutes consent to the website's tracking practices. However, users do not read or understand the lengthy privacy policies, and membership in the NAI or participation in a seal program does not accurately indicate a website's practices. Although a variety of opt-out mechanisms exist, they are cumbersome and ineffective. Accordingly, if users somehow receive effective notice, their only choice is to desist from using the majority of websites.[85] In other words, users cannot effectively prevent unwanted online profiling.

81. Torpey, *supra* note 73.

82. *DoNotTrack FAQ*, MOZILLAWIKI, https://wiki.mozilla.org/Privacy/Jan2011_DoNotTrack_FAQ (last modified Jan. 24, 2011, 21:56).

83. For instance, Microsoft ceased development of Internet Explorer for Mac in 2003, at which time IE5 was current. Jim Dairymple, *Microsoft Drops Development of IE for Mac*, PCWORLD (June 13, 2003, 6:00 PM), http://www.pcworld.com/article/111158/microsoft_drops_development_of_ie_for_mac.html.

84. 2010 REPORT, *supra* note 33, at 65–66.

85. *Cf.* Shaun A. Sparks, Comment, *The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumer Personal Data*, 18 DICK. INT'L L. ANN. 517, 549 (2000) (stating optimistically that "[o]nline businesses . . . will compete in the arena of privacy service in the same manner in which they compete on terms such as price").

C. *There Are Limited Remedies Available for Harms Resulting from Online Profiling*

Even as users lack effective means to prevent online profiling, only limited remedies are available once online profiling has occurred. Courts have resisted application of existing legislation to cookies. State and national legislatures have not yet passed regulations that would specifically regulate online profiling, and recent proposals face numerous obstacles. Until quite recently, the FTC has been noticeably hands-off, emphasizing principles to guide industry self-regulation and future legislation. In short, consumers lack adequate remedies.

1. Existing Legislation

None of the three pieces of federal legislation most likely to protect users from online profiling—the Electronic Communications Privacy Act, the Federal Wiretap Act, and the Computer Fraud and Abuse Act—are applicable to online profiling. In the four cases directly addressing the applicability of these statutes to online tracking mechanisms, courts have consistently dismissed claims due to consent between websites and advertisers and damage thresholds.

The Electronic Communications Privacy Act (ECPA) makes it an offense to access without authorization "a facility through which an electronic communication service is provided" and thus obtain "access to a wire or electronic communication while it is in electronic storage in such system."[86] This provision has not protected users from online profiling because courts have held that ad servers fall within a statutory exception, stating that the relevant section "does not apply with respect to conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[87] In *In re DoubleClick Inc. Privacy Litigation*, a federal district court held that, within the exception, "user" refers to websites or servers. Thus, the exception applies to conduct authorized by websites rather than conduct authorized by individual users.[88] The court then held that, given its commercial relationships with affiliated websites, those sites had authorized DoubleClick to access the

86. 18 U.S.C. § 2701(a) (2006).

87. 18 U.S.C. § 2701(c)(2).

88. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 509 (S.D.N.Y. 2001). *But see In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1277 (C.D. Cal. 2001) ("If the thrust of Defendant's 'third party' contention is that it was authorized to access data in Plaintiff's computer, the court must reject it as it directly conflicts with Plaintiffs' allegations that Defendant was not so authorized, which allegations the court must accept as true for the purposes of a *Rule 12(b)(6)* motion to dismiss."). However, the result in *Intuit* may be due to the procedural posture—motion to dismiss—rather than the inherent strength of the argument. *See In re* Toys R Us, Inc., Privacy Litig., No. C 00-2746 MMC, 2001 U.S. Dist. LEXIS 16947, at *13 (N.D. Cal. Oct. 9, 2001).

GET, POST, and GIF communications sent by the plaintiffs to the website.[89] As a result DoubleClick's access to users' GET, POST, and GIF communications fell within the statutory exception because they were authorized by the websites. A similar result was reached in a case in which plaintiffs filed a suit against Avenue A, an advertising network, alleging that Avenue A was not authorized by websites that did not contract directly with Avenue A but rather were re-routed to its servers by DoubleClick. The court held that ECPA does not apply to parties to whom communications are re-routed, and so it was sufficient that websites had initially granted authorization to DoubleClick.[90]

The court in *DoubleClick* further held that ECPA does not even apply to cookies because they are not "electronic storage." Electronic storage is "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[91] The court held that the requirement for temporary storage was not met because users' computers store cookies for indefinite periods;[92] the second prong was not met because users are not "electronic communication service[s]."[93] Even if cookies did fall within ECPA's provisions, the court held that access to the identification numbers associated with each cookie was internal communication within DoubleClick, and so DoubleClick required no authorization to access them, though they were stored on users' hard drives.

Courts have also held that the Federal Wiretap Act is inapplicable to online tracking. The Federal Wiretap Act provides a private right of action against the interception of electronic communications.[94] The plaintiffs in *DoubleClick* argued that DoubleClick intercepted communications between themselves and the websites they visited. However, an exception to the Federal Wiretap Act provides that interception is not unlawful where the interceptor "is a party to the communication or

89. *DoubleClick*, 154 F. Supp. 2d at 511. GET and POST queries allow users to type information, such as search queries and personal information, into websites. GIF tags are web beacons.

90. Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001).

91. 18 U.S.C. § 2510(17) (2006).

92. *DoubleClick*, 154 F. Supp. 2d at 511–13; s*ee also Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *11 ("Just as in *DoubleClick*, plaintiffs here allege that the cookies at issue remain 'indefinitely' on their computers . . . and do not allege that the cookies are incidentally stored in plaintiffs computers while awaiting final transmission to another location.").

93. *DoubleClick*, 154 F. Supp. 2d at 511; *see also Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *18 ("While the complaint clearly alleges that plaintiffs did not authorize Coremetrics to access their E91communications within websites, the statutory exception set forth in § 2701(c)(2) is applicable as long as one party to a communication provides consent.").

94. 18 U.S.C.S. § 2511(a) (Lexis Nexis 2011).

where one of the parties to the communication has given prior consent to such interception."[95] The court in *DoubleClick*, applying an analysis similar to its approach to ECPA, held that the parties to the communications were the websites and DoubleClick—not the plaintiffs—and the websites had granted authorization.[96]

Finally, although the Computer Fraud and Abuse Act (CFAA), broadly speaking, prohibits unauthorized access to protected computers,[97] the limited availability of private rights of action makes it inapplicable to tracking. The CFFA only allows civil actions against a party who "intentionally accesses a protected computer without authorization and, as a result of such conduct, recklessly causes damage."[98] Damage, in turn, "means any impairment to integrity or availability of data, a program, a system, or information."[99] Furthermore, the offense must have caused damages "aggregating at least $5000 in value."[100] As an initial matter, a properly functioning tracking mechanism will not impair data, programs, systems, or information; if it did, it would probably prevent a user from engaging in the activities it is meant to track. Assuming, that it did cause such damage, plaintiffs would have to overcome the hurdle of showing recklessness. Finally, plaintiffs would have to meet the damages threshold. Few did so successfully under an earlier version of the statute, which defined "damage" as "any impairment to the integrity or availability of data, a program, a system, or information that . . . causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals."[101] For instance, the court in *DoubleClick* held that the plaintiffs could aggregate damages across victims and over time but only with respect to a single act.[102] Aggregation across victims did not help the plaintiffs because DoubleClick committed different acts

95. 18 U.S.C.S. § 2511(2)(d).

96. *DoubleClick*, 154 F. Supp. 2d at 514; *see also* Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) ("It is implicit in the web pages' code instructing the user's computer to contact Avenue A, either directly or via DoubleClick's server, that the web pages have consented to Avenue A's interception of the communication between them and the individual user."); *Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *24–25.

97. 18 U.S.C.S. § 1030(a) (LexisNexis 2011).

98. 18 U.S.C.S. § 1030(a)(5)(B); *see also* 18 U.S.C.S. § 1030(g) ("A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."); 18 U.S.C. § 1030(c)(4)(A)(i) ("The punishment for an offense under subsection (a) or (b) of this section is . . . except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of . . . an offense under subsection (a)(5)(B).").

99. 18 U.S.C.S. § 1030(e)(8).

100. 18 U.S.C.S. § 1030(c)(4)(A)(i)(I).

101. 18 U.S.C. § 1030(e)(8) (2000) (amended 2001).

102. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 523–24 (S.D.N.Y. 2001).

each time it accessed cookies on the millions of different computers.[103] Even if plaintiffs aggregated the repeated access of one cookie on one user's computer across time, the court was not convinced that the harm suffered by each plaintiff was valued at or above $5000.[104]

2. Proposed Legislation

New legislation has not filled the gap left by ECPA, the Wiretap Act, and CFAA. No legislative body has passed regulations that specifically apply to online profiling, although several have offered proposals. A New York bill would prohibit the collection of personally identifiable information ("PII")[105] without consent. It would also require an opt-out option regarding the collection of non-PII, clear display of privacy policies on advertisers' home pages, and clear notice of advertisers' practices by publishers. The bill allows the attorney general to bring actions for violations. It imposes a fine of up to $250 per violation, and the court may triple this fine upon finding a pattern or practice of either collecting PII without consent or failing to allow users to opt out of the collection of non-PII.[106]

At the national level, Representative Rush has proposed a bill that would set standards for notice-and-choice procedures, including an opt-out option for covered information and a requirement of express consent regarding sensitive information. The bill grants the FTC rulemaking authority with respect to the accuracy of data, allowing consumers limited access to their data, and standards regarding data security, retention, and accountability. The bill would create a private right of action but also

103. *Id.* at 524; *cf. In re* Toys R Us, Inc., Privacy Litig., No. C 00-2746 MMC, 2001 U.S. Dist. LEXIS 16947, at *36 (N.D. Cal. Oct. 9, 2001) (aggregating plaintiffs' claims where "defendants caused an identical file to be implanted in each of the plaintiffs' computers, resulting in damages of a uniform nature").

104. *DoubleClick*, 154 F. Supp. 2d at 525–56; *see also* Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001) ("Plaintiffs have not shown any facts that prove an aggregate damage of over $5,000 for any single act of the Defendant, from either the initial placement of an Avenue A cookie or a subsequent accessing of this cookie."); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001) (holding that plaintiffs were unable to meet the damages requirement).

105. PII is information that "by itself, can be used to identify, contact or locate a person." Online Consumer Protection Act, Gen. Assemb. B. A4809, 2011 Leg., 234th Reg. Sess. (N.Y. 2011); *see also* NETWORK ADVERTISING INITIATIVE, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT 5 (2008) ("PII includes . . . any other data used or intended to be used to identify, contact or precisely locate a person."). Note, however, that numerous commentators have questioned the merits of a distinction between PII and non-PII. *See, e.g.*, 2009 REPORT, *supra* note 2, at iii; Ohm, *supra* note 62.

106. N.Y. Assemb. B. A4809. The bill is currently under review by the Consumer Affairs and Protection Committee. *Legislative Detail: NY Assembly Bill 4809 – 2011 General Assembly*, LOBBYIST, http://e-lobbyist.com/gaits/NY/A04809 (last visited Mar. 8, 2011).

create a "safe harbor" for companies that participate in an FTC-approved self-regulatory program. The bill also permits enforcement by the FTC and states' attorneys general.[107]

Representatives Boucher and Stearns have offered a more limited draft. They would require notice-and-choice procedures that permit consumers to opt out of the sharing of covered information and require consumers to grant affirmative opt-in consent regarding sensitive information. Their draft also creates more limited standards regarding data accuracy and security. They would permit enforcement by the FTC and states' attorneys general but would not allow a private right of action.[108]

The fate of these bills is unclear. With the exception of the Children's Online Privacy Protection Act, relevant legislative proposals have all failed to pass.[109] If successfully passed, any future national regulatory scheme might preempt state legislation such as New York's.[110] In the wake of recent developments including the FTC's and Department of Commerce's new reports[111] and Representative Boucher's failure to win reelection,[112] the current proposals are likely to be both outdated and dead in the water.

3. The FTC's Role

The FTC is "empowered and directed to prevent persons, partnerships, or corporations . . . from using . . . unfair or deceptive acts or practices in or affecting commerce."[113] Under that mandate, the FTC has considered matters related to online privacy through public workshops and hearings since 1995.[114] Nonetheless, until recently, the FTC's approach could be best characterized as "wait and see."

In 1998, the FTC released a report on online privacy. It identified five "fair information practices"—notice, choice, access, security, and enforcement—and found that the majority of online businesses had not adopted them. The FTC concluded that some added incentives were

107. Best Practices Act, H.R. 5777, 111th Cong. (2010).

108. Boucher/Stearns Discussion Draft, 111th Cong. §§ 8(b), 9 (2010) (on file with author).

109. *See, e.g.*, H.R. 1263, 109th Cong. (2005).

110. For example, the Best Practices Act would preempt state laws governing "covered information." H.R. 5777 § 605(a).

111. 2010 REPORT, *supra* note 33; DEP'T OF COMMERCE, *supra* note 10.

112. *2010 Rick Boucher Elections Results*, POLITICS DAILY (Nov. 9, 2010, 5:37 PM), http://www.politicsdaily.com/tag/Rick+Boucher/.

113. 15 U.S.C. § 45(a)(1) (2006).

114. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter "1998 REPORT"].

necessary to encourage industry self-regulation but did not recommend legislation, except with respect to children under twelve.[115]

In 2000, the FTC addressed the specific issue of online profiling. The FTC reviewed self-regulatory principles proposed by the NAI and found that they "reasonably implement the fair information practice principles."[116] Nonetheless, the FTC recommended "backstop legislation" to address those actors not reached by the NAI. Legislation would create basic standards regarding collection and use of information gathered online and intended for profiling, create an implementing agency with rule-making and enforcement authority, and grant a safe harbor to parties adopting self-regulatory principles that implement the fair information practices.[117]

The FTC turned its attention to online profiling again in 2007 following petitions from several organizations and its investigation into the merger between Google and DoubleClick.[118] After a period of meetings, proposals, and public comment, the FTC released a new set of four self-regulatory principles: transparency and consumer control, reasonable security and limited data retention for consumer data, affirmative express consent for material changes to existing privacy promises, and affirmative express consent to (or prohibition against) using sensitive data for OBA.[119]

These principles set very loose standards. For example, the principles do not apply to "first party" or "intra-site" online profiling, and the definition of "first party" is very broad.[120] It may include affiliated companies if the relationship is "sufficiently transparent and consistent with reasonable consumer expectations."[121] It may even include sharing data with "third-party service providers in order to deliver ads . . . provided there is no further use of the data by the service providers."[122] In addition, the FTC downplayed the importance of "enforcement," demoting it from fair information principle[123] to a one-and-a-half sentence mention in the conclusion,[124] and the report did not discuss its removal from the list of principles. Finally, although the report addressed self-regulatory princi-

115. *Id.*
116. 2000 REPORT PART 2, *supra* note 7, at 4.
117. *Id.* at 10–11. No such legislation was ever passed.
118. 2009 REPORT, *supra* note 2, at 8–9.
119. *Id.* at 46–47.
120. *See* Stallworth, *supra* note 2, at 488 (characterizing the change as an "unprecedented limitation to the scope of the proposed guidelines").
121. 2009 REPORT, *supra* note 2, at 28 n.59.
122. *Id.* at 28 n.58.
123. 1998 REPORT, *supra* note 114, at 10.
124. 2009 REPORT, *supra* note 2, at 47.

ples, the FTC did not take the opportunity to reiterate its previous call for "backstop legislation."

Along with its issuance of comments and guidelines, the FTC has brought numerous cases against businesses that failed to protect consumers' personal information.[125] Despite the FTC's arguable successes, its mandate to consumer protection and not consumer privacy fundamentally limits it.[126] Thus, many matters regarding online profiling fall outside of the FTC's authority. For instance, Google posts both a privacy policy and a simplified summary that avoids "legalese," both practices the FTC promotes; however, the policy in practice provides few limits on OBA. So long as Google complies with its own policy, its practices regarding OBA are outside of the FTC's enforcement scope.[127] Furthermore, the FTC's settlements with offenders do not bind other parties and "are often no more than slaps on the wrist."[128]

In short, despite its numerous studies, meetings, reports, and comments, the FTC's results are ultimately limited to ever-loosening principles regarding self-regulation and unsuccessful calls for legislation. Meanwhile, its investigations have neither remedied nor deterred harmful profiling practices.

D. *Regulation Is Necessary to Protect Users*

This section has established that online profiling is a harmful practice from which users are unable to effectively protect themselves and for which there are no legal remedies. Because industry self-regulation under the notice-and-choice regime has proven inadequate, legislation is necessary.

Advertisers and others argue that legislation is undesirable because it would inhibit economic growth.[129] Online advertising's economic benefits include subsidization of online content and lower barriers to market entry for new businesses.[130] A study sponsored by the Interactive Advertising Bureau (IAB) even argues that the jobs of about two percent of Americans in 2009 existed solely because of the "advertising supported

125. 2010 REPORT, *supra* note 33, at 10–11.

126. Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 308 (2003).

127. Stallworth, *supra* note 2, at 484–87.

128. DeVries, *supra* note 126, at 308.

129. PONEMON INST., ECONOMIC IMPACT OF PRIVACY ON ONLINE BEHAVIORAL ADVERTISING 6 (2010), *available at* http://www.betteradvertising.com/OBA_paper.pdf.

130. Letter from J. Trevor Hughes, Exec. Dir., Network Adver. Initiative, to Donald S. Clark, Sec'y, Fed. Trade Comm'n 6–7 (Oct. 19, 2007), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf; Letter from Michael Zaneis, Vice President of Pub. Policy, Interactive Adver. Bureau, to Donald S. Clark, Sec'y, Fed. Trade Comm'n 2–3 (Oct. 19, 2007), *available at* http://www.iab.net/media/file/IAB-Behavioral_advertising_comments.pdf.

Internet."[131] These figures are misleading because online profiling represents only a small percentage of online advertising. Specifically, although advertising subsidizes much online content and supports a large industry, these benefits do not derive from online profiling in particular. One recent study found that the ninety surveyed companies spent an average of only 11.7% of their online advertising budgets on OBA.[132] Furthermore, if advertisers were unable to target users through profiling, they likely would redirect at least some portion of the funds currently devoted to OBA to other online advertising avenues, such as delivering advertisements tied to search results or the general content of a webpage. Current practices may even be harmful to innovation because they cause economic loss by undermining consumer trust, which inhibits use of new services.[133]

Advertisers also argue that users would not pay a market rate for Internet content if it were not free, which advertisers contend would be the inevitable result if websites could no longer sell ad space. A study by the IAB purports to support this argument, finding that the value American and European consumers obtain from web services is six times greater than what consumers would spend to avoid advertising and its attendant privacy risks.[134] However, a recent Gallup poll shows that a sizeable majority of consumers believe that "free access is not worth the invasion of privacy involved,"[135] demonstrating that the argument is not as clear-cut as advertisers argue.

The advertising industry and others further contend that legislation would inhibit technical innovation.[136] It is true that unregulated development of online profiling and OBA has led to several new technologies and tools, such as the complex algorithms that drive RTB and the Evercookie. However, bald assertions that regulation will inhibit innovation are not arguments against regulation but rather a statement of regulation's possible effect. It may even have a positive effect; more and better tracking technologies are not necessarily desirable. Furthermore, the de-

131. HAMILTON CONSULTANTS ET AL., ECONOMIC VALUE OF THE ADVERTISING-SUPPORTED INTERNET ECOSYSTEM 4 (2009), *available at* http://www.iab.net/media/file/Economic-Value-Report.pdf.

132. PONEMON INST., *supra* note 129, at 4–5.

133. DEP'T OF COMMERCE, *supra* note 10, at vi.

134. IAB EUR., CONSUMERS DRIVING THE DIGITAL UPTAKE: THE ECONOMIC VALUE OF ONLINE ADVERTISING-BASED SERVICES FOR CONSUMERS 5 (2010), *available at* http://iabeurope.eu/media/39559/whitepaper%20_consumerdrivingdigitaluptake_final.pdf.

135. Lymari Morales, *U.S. Internet Users Ready to Limit Online Tracking for Ads*, GALLUP (Dec. 21, 2010), http://www.gallup.com/poll/145337/Internet-Users-Ready-Limit-Online-Tracking-Ads.aspx.

136. *See, e.g.*, Svetlana Milina, Note, *Let the Market Do Its Job: Advocating an Integrated Laissez-Faire Approach to Online Profiling Regulation*, 21 CARDOZO ARTS & ENT. L.J. 257, 272 (2003).

crease in resources spent on development of tracking technologies may allow for an increase in resources spent elsewhere. Unregulated online profiling does not necessarily lead to a net increase in innovation but rather to a trade-off in the nature of innovation.

Online profiling presents a classic case for regulation: it is a harmful practice from which consumers cannot protect themselves and for which there is no existing remedy. The advertising industry has offered three flawed arguments against regulation of online profiling. First, the advertising industry argues that a reduction in OBA will lead to a corresponding reduction in subsidized Internet content. However, a decrease in OBA will not spell the end of the ad-supported internet because OBA constitutes only a small portion of online advertising budgets. Second, the advertising industry argues that users like receiving OBA. However, surveys show that users do not agree that the benefits of ad-subsidized Internet content outweigh the loss of privacy. Finally, the advertising industry argues that innovation of some unspecified nature will suffer. While innovation in the field of online profiling and OBA may decrease, other forms of innovation will probably not. Accordingly, these objections do not overcome the need for regulation.

III. THE 'DO NOT TRACK' MECHANISM

The FTC has characterized its approach from 1995 through 2010 as focusing on two elements: notice-and-choice and harm to consumers. Setting a markedly different tone, the FTC acknowledges in its most recent review that the notice-and-choice model simply has not worked with respect to online profiling. The FTC cites many of the problems discussed above: ineffective industry self-regulation, lack of consumer awareness, and opaque privacy settings, among others.[137]

To avoid these problems, the FTC proposes a "more uniform and comprehensive consumer choice mechanism for online behavioral advertising," now referred to as the 'do not track' option.[138] The FTC suggests that this option could function similarly to a persistent cookie on a user's browser that informs visited sites whether or not the user permits tracking or the delivery of targeted advertising.[139] The remainder of this

137. 2010 REPORT, *supra* note 33, at 64–66.

138. *Id.* at 66.

139. *Id.* Although the FTC describes the 'do not track' mechanism as similar to a persistent cookie, it appears that the purpose is not to block all cookies, which would inhibit users from enjoying many websites, but instead to inform parties attempting to install cookies that the user does not wish to be tracked.

section suggests ways in which this could be implemented in order to give consumers effective options regarding online profiling.

A. *Design of the 'Do Not Track' Mechanism*

It appears that the FTC would require any party not acting under "commonly accepted" practices[140] to respect the user's tracking preferences. Commonly accepted practices include first-party marketing, which the FTC proposes should "include only the collection of data from a consumer with whom the company interacts directly for purposes of marketing to that consumer."[141] Thus, many business affiliates and all third parties, other than service providers, would be unable to track users who opt out through the 'do not track' mechanism.[142] This standard should be supported, with the exception that tracking by business affiliates, even those whose "affiliate relationship is clear to consumers through common branding or similar means,"[143] should not be permitted. Tracking by affiliates opens too many questions and loopholes regarding whether affiliations are apparent to consumers.

The 'do not track' mechanism should be implemented through legislation rather than voluntary industry compliance. The FTC suggests that "robust, enforceable self regulation" is an option. The Department of Commerce suggests that such a standard would be effective if there were proper incentives for compliance, such as enhanced FTC enforcement, provision of safe harbors for the adoption of certain minimal standards, and increased pressure from Executive officials on industry to develop standards.[144] This approach is inadequate; the advertising industry has shown that it cannot be relied upon to design and implement an effective mechanism that will protect consumer privacy. Even under the more lenient notice-and-choice regime, the FTC found that self-regulatory efforts had "fallen short,"[145] and the Department of Commerce noted that the NAI principles are the "*only* significant example of a voluntary code of conduct."[146] The reason is simple: the online advertising industry enjoys greater profits from targeted advertising than other forms of advertising, and so it is in the industry's interest to make it difficult for consumers to prevent profiling.[147] A centralized and disinterested stan-

140. *Id.* at 53–54.
141. *Id.* at 55.
142. *Id.*
143. *Id.*
144. DEP'T OF COMMERCE, *supra* note 10, at 42.
145. 2010 REPORT, *supra* note 33, at 64.
146. DEP'T OF COMMERCE, *supra* note 10, at 42 (emphasis in original).
147. It is not certain that the online advertising industry would be solely responsible for the design or implementation of a 'do not track' mechanism. However, it is likely that a party

dard-setting body, whether it is Congress acting through specific legislation or a government agency acting with rule-making authority, would minimize self-interested decisions by the industry. In order to maintain flexible standards that can adapt to developing technologies, Congress should establish basic standards and endow an agency, likely the FTC, with rule-making authority to implement those standards.[148]

The basic standards should include a requirement that all Internet applications provide a 'do not track' mechanism. This requirement should extend to browsers, mobile applications, and other means of accessing the Internet.[149] An ever-increasing range of devices and technologies enable online activities, and exempting these growing fields would leave a major gap in the legislation. Through the remainder of this section, "Internet application" will refer to any means of accessing the Internet.

Any Internet application installed or updated after the legislation takes effect should automatically display the mechanism to users the first time it is opened.[150] This will ensure that consumers are aware of the options that exist, making it a valuable supplement to any consumer education campaign. The mechanism should remain easily accessible thereafter.

The mechanism must present three options: allow all tracking, allow tracking by certain companies, and deny all tracking. Delivery of OBA is not, in and of itself, a bad thing; the harms identified above stem from lack of user control over their information and an inability to escape the "box." Allowing users to select the companies that can track them would narrowly address the harms associated with unrestricted tracking by granting users control over their information. It would also meet users' desires: a recent Gallup poll indicates that forty-seven percent of Americans want to allow tracking by advertisers of their choice.[151]

---

designing such a mechanism would find it necessary to consult with the advertising industry. Furthermore, companies might own both browsers and advertising companies—Google owns both Chrome and DoubleClick, for example—giving them an incentive to hinder their browsers' compliance.

148. It is important that Congress create these standards. The Department of Commerce calls for the creation of a "Privacy Policy Office" (PPO). The PPO would work with stakeholders to propose new codes, which would undergo comment and review periods. If approved, the FTC would enforce the code; if the process does not result in an enforceable code, the PPO would recommend FTC rules or legislation. DEP'T OF COMMERCE, *supra* note 10, at 48. This would simply insert an extra step into the development of rules, delaying the creation of important standards. Adequate opportunities for comment and consensus-building exist in current notice-and-comment periods.

149. The FTC questions whether this is necessary. 2010 REPORT, *supra* note 33, at 68–69.

150. It is unclear whether there is a way to require users to update existing browsers.

151. Morales, *supra* note 135.

Allowing users to select which companies may track them does put some burden on users to learn about the companies' practices, and so it is necessary to take a number of complementary steps to prevent a de facto return to the current, ineffective "notice-and-choice" regime. The Department of Commerce has called for a comprehensive new approach to privacy, which might address these concerns. Among other recommendations, the report calls for greater transparency through shorter and clearer disclosures, user-friendly interfaces, and "Privacy Impact Assessment specifications," which would provide users with "a road map to an organization's collection and use of personal information."[152] However, disclosure alone is not enough. An entity that states it will do anything it likes with users' information is hardly protecting privacy, though it is providing full disclosure.[153] The Department of Commerce calls for purpose specification and use limitation. "Purpose specification" would require companies to state with specificity the purposes for which they collect information; "use limitation" prohibits companies from using gathered information for any other purpose.[154] Finally, the Department of Commerce suggests that audits could verify—and provide incentives for—compliance with purpose specification and use limitations.[155] Taken together, these requirements would present users with clear explanations of how and why companies collect information, what they intend to do with it, and whether they adhere to their statements. This is an effective "notice" regime.

As for "choice," users could simply disallow tracking by those companies whose practices are distasteful. While most users will not have the time to familiarize themselves with each company's practices, users may have the option to rely upon lists assembled by privacy advocacy groups,[156] who would have the time and resources to review companies' practices. Such an option is not objectionable when accompanied by a choice to block *all* tracking, not merely tracking by companies found on third-party lists.[157]

Note that the mechanism should allow users to consent to tracking only by specified companies. The mechanism should not allow users to agree to tracking based on specified categories of interests or data type. Such standards would be unworkable. For example, if a user allows

152. DEP'T OF COMMERCE, *supra* note 10, at 36.

153. *Id.* at 38.

154. *Id.* at 38–40.

155. *Id.* at 40.

156. Tanzina Vega, *Microsoft, Spurred by Privacy Concerns, Introduces Tracking Protection to Its Browser*, N.Y. TIMES, Dec. 7, 2010, at B6, *available at* http://www.nytimes.com/2010/12/08/business/media/08soft.html?_r=1&hpw.

157. *See supra* text accompanying note 80.

tracking regarding gardening, may trackers gather information about the user from any sites related to gardening? If so, may trackers collect only information providing more specific details regarding the user's interest in gardening, such as whether they have an orchard or a houseplant? May trackers identify users on websites not related to gardening in order to display advertising related to gardening? Defining other categories of permitted tracking is similarly unworkable. Allowing blanket collection of non-sensitive information would invite disputes regarding the definition of "sensitive."[158] Blanket collection of non-PII information would be an empty standard, as all information is nearly-PII; aggregating even small amounts of non-PII can produce PII information.[159] Allowing users to permit collection of discrete pieces of data, such as their location, would invite exploitation of users who do not understand the ways in which information may be aggregated. With respect to any of these options, it is not clear with whom trackers may share gathered information and whether there are limits on recipients' use of that information. In short, allowing limited tracking based on user-specified categories would appear to open more doors than it closes or, at the very least, to invite unmanageable difficulties in defining terms and setting limits.

In addition, the mechanism should not allow users to consent to third-party tracking while they are visiting certain sites. Such a system would limit user control because users would not necessarily know which third-party trackers were present. It would also give websites an incentive to require users to allow tracking in order to use their sites, further undermining user control.

In presenting these options to users, the mechanism should be brief and readily understandable. The more options the mechanism provides, the more confusing it may be.[160] An acceptably simple yet accurate system might present a single screen with a one-paragraph description of online profiling and links to more specific information. There should be three boxes following this paragraph: one that permits all tracking, one that permits tracking by certain companies, and one that does not permit any tracking. If a user indicates a desire to permit tracking by certain companies, the user should be presented with a page allowing him to select individual companies or to select groups of companies based upon

158. *Compare* Best Practices Act, H.R. 5777, 111th Cong. § 2(8) (2010) (including a broader range of sensitive information, such as sexual behavior in addition to sexual orientation, but requiring that it "relate directly" to the characteristic in question), *with* Boucher/Stearns Discussion Draft, 111th Cong. § 2(10) (2010) (on file with author) (including a narrower range, such as sexual orientation but not sexual behavior, but only requiring that the information "relate" to the characteristic in question). The FTC continues to seek input on how to adequately define "sensitive information." 2010 REPORT, *supra* note 33, at 61.

159. Ohm, *supra* note 62, at 1719–20.

160. *See supra*, notes 76–78 and accompanying text.

their compliance with certain privacy practices or approval by privacy advocacy groups. The FTC or other rule-making body would have the authority to set specific standards to accomplish this.

Websites will thwart the purpose of a 'do not track' mechanism if they are able to deny access to users who did not permit tracking, since necessary or popular sites might then compel users to permit tracking in order to access the sites. Therefore, websites should not be permitted to block users who do not allow tracking or to condition full access on users' consent to tracking by certain companies.[161] Websites should not suffer a significant loss of revenue from this, as they are still free to display context- or search-based advertising, as well as targeted advertising to those users who allow it. If, however, websites do choose to charge users who have opted out of tracking, the websites may not charge unreasonable fees in order to coerce users into permitting tracking. Coercion may be determined by reference both to the amount of money charged and interference with the browsing process, such as requiring users to complete a separate transaction each time they navigate to a different page within the site.

B. *Enforcement of the 'Do Not Track' Mechanism*

There must be a way to ensure compliance with the 'do not track' mechanism. The FTC apparently confines its envisioned enforcement to technical tools that limit websites' abilities to track objecting users.[162] This is inadequate; there must be some means of obtaining legal and equitable remedies against parties that do not comply, or the industry will continue to be "the fox guarding the hen-house."[163]

The FTC ought to retain its authority over unfair and deceptive trade practices with respect to the 'do not track' mechanism. This enforcement authority should apply against both tracking that evades the 'do not track' mechanism and browsers whose mechanisms do not meet basic standards.

Legislation should permit states' attorneys general to seek damages and injunctions against further violations. Internet applications should be liable if they know that their mechanism is ineffective but do not correct it; compliance with relevant FTC regulations will act as a safe harbor.

161. *Cf.* H.R. 5777 § 103(f) (allowing full access to be contingent upon permission to collect covered information).

162. 2010 REPORT, *supra* note 33, at 64.

163. Ethan Hayward, Note, *The Federal Government as Cookie Inspector: The Consumer Privacy Protection Act of 2000*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y 227, 233 (2001); *see also* DEP'T OF COMMERCE, *supra* note 10, at 43 (suggesting that if a safe harbor protects companies whose privacy policies meet certain standards, "the 'carrot' offered by a safe harbor has force only if there is a corresponding 'stick'").

Parties who track users despite their use of the 'do not track' mechanism should face strict liability. This will encourage browsers to ensure that their mechanisms are effective but will not deter innovation and entry into the market.

Damages should be awarded on a per-violation basis with the option to triple them if a pattern or practice of violation is shown.[164] If any cap is set, it should be high enough that it will still have a deterrent effect on actors that are worth billions of dollars, such as Google.[165] A cap proportional to the parties' online advertising budget might be appropriate.

Private rights of action would be of limited use, as many consumers will not be aware of impermissible tracking and the injury suffered may not be large enough to bring suit. Nonetheless, private actions should be permitted so as to allow users who have been injured to vindicate their right to prevent tracking. This would also compensate for under-enforcement by federal and state agencies.[166] Finally, it would provide an opportunity for privacy advocacy groups to intervene on behalf of individuals.

CONCLUSION

Online profiling is a dangerous practice. It permits the collection of vast quantities of information regarding largely unsuspecting or unwilling users, and there are currently no adequate safeguards to protect them. This Note focused on the harms stemming from lack of consumer knowledge, consent, and ability to employ self-protective measures. The FTC's 'do not track' mechanism has the potential to address many of these concerns, but it will not be effective unless implemented by legislation that mandates certain basic standards and supports those standards with effective enforcement mechanisms.

Of course, presenting users with options to avoid some or all tracking will only be effective if users are able to make informed decisions. Given the pervasiveness of the Internet, users are almost shockingly ignorant of online profiling and privacy practices.[167] Requiring Internet

164. This is the method followed in New York's Online Consumer Protection Act, Gen. Assemb. B. A4809, 2011 Leg., 234th Reg. Sess. (N.Y. 2011).

165. The $5 million cap proposed in the Best Practices Act seems too small for this reason. H.R. 5777 § 603(b)(3). One survey found that seventy percent of Americans believe a company that purchases or uses someone's information illegally should be fined more than $2500, although it is unclear whether this question refers to a single violation or repeated ones. Turow et al., *supra* note 47, at 23. In addition, a substantial minority (thirty-eight percent) believes executives should face criminal liability. *Id.*

166. DEP'T OF COMMERCE, *supra* note 10, at 29.

167. Turow et al., *supra* note 47, at 19–22.

applications to present users with a simple list of options will at least encourage users to make a purposeful choice, but it will not necessarily provide the background they need. Because users will be able to allow some or all tracking, they must know enough about the harms and alleged benefits of online profiling to make an informed decision regarding the degree of protection of their privacy online. Accordingly, consumer education campaigns should complement the 'do not track' mechanism.[168]

The harms of online profiling extend beyond those discussed in this Note. The industry depends upon the accumulation, storage, and dissemination of vast quantities of information, an alarming practice given the current lack of standards regarding data retention and data security. Future legislation should make the 'do not track' mechanism just one part of a comprehensive plan to protect users' information. This can all be accomplished without destroying the advertising-supported Internet, to which online profiling and OBA contribute only a small percentage.

168. 2010 REPORT, *supra* note 33, at 78–79; DEP'T OF COMMERCE, *supra* note 10, at 48.