Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 27 | Issue 1 Article 2

2010

Balancing Consumer Privacy with Behavioral Targeting

Dustin D. Berger

ARTICLES

BALANCING CONSUMER PRIVACY WITH BEHAVIORAL TARGETING

Dustin D. Berger†

Abstract

Behavioral targeting is the emerging practice of collecting information about consumers' behavior and using that information to customize an advertisement or other service for the consumer. This article first describes the practice and technology of behavioral targeting in its various forms. Second, it aims to identify how this emerging technology might benefit and harm consumers, and to understand how harms occur. Third, it overviews the FTC's self-regulatory principles and a variety of other proposals to strengthen regulations to prevent harm to consumers and concludes that the proposed approaches do not give consumers the right information to effectively allow them to intelligently manage the risk of harm. Therefore, the article proposes a regime of broad mandatory regulation combined with an audit requirement to address the root causes of potential harm. The article argues that this approach will aid consumers in making informed decisions about their participation in activities that involve behavioral targeting.

INTRODUCTION

In a 2006 article, the *New York Times* described how easy it was to discover the identity of a person based on the information that a website had collected about her. Two *Times* reporters obtained a set of publicly available data describing the Internet searches of America Online (AOL) customers.[1] Although the data contained no

† Dustin D. Berger (LL.M. Candidate 2011, J.D. 2009, M.B.A. 2003, B.S. Comp. Sci. 2001) was formerly the chief technology officer for the Town of Parker, Colorado. He thanks Professor John Soma and Michael Smith for their invaluable feedback on this article. He also thanks Jeremiah Mashore, without whom this article would not have been possible.

1. Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A2, *available at*

information that directly identified the persons who had performed the searches, the reporters were nevertheless able to use the search data to identify and interview one of the customers.[2]

Thelma Arnold, a sixty-two-year-old widow who lives in Lilburn, Georgia, conducted Internet searches for "60 single men," "dog that urinates on everything," and "numb fingers."[3] When the reporters located her, she confirmed that the searches were indeed hers.[4] Ms. Arnold, who was identified in the search data only by the number 4417749 and the contents of the searches themselves, also conducted a number of searches related to medical conditions, which, she explained to the *New York Times* reporters, she often does on behalf of friends.[5] While Ms. Arnold was indignant about AOL's disclosure of her searches, and said she intended to drop her AOL service,[6] the damage to Ms. Arnold's privacy had been done. Now the readers of the *New York Times* know of Ms. Arnold's search for "60 single men." Both Ms. Arnold and AOL were fortunate that the information the *New York Times* was able to put together was only embarrassing for Ms. Arnold.

For some time, websites and Internet service providers (ISPs) have been compiling profiles about their customers.[7] These profiles allow websites and ISPs to serve advertisements and other services that are targeted to their customers' interests.[8] Like the profile AOL constructed of Ms. Arnold, these profiles usually do not contain any information, such as a name, address, or social security number, that directly identifies the profiled customer.[9] Nevertheless, profilers are capturing and aggregating more information about consumers, and, consequently, consumers' profiles are becoming so detailed that it is increasingly possible to discern the identities of the consumers from the data in the profiles.[10] Because the profiled consumer can be identified, the consumer may be embarrassed if his or her Internet behavior is matched to his or her identity. And, many consumers

---

http://www.nytimes.com/2006/08/09/technology/09aol.html.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING I-II (2009) [hereinafter PRINCIPLES].

8. *Id.*

9. *See* Barbaro & Zeller, *supra* note 1.

10. *Id.*

would be understandably indignant at the detailed picture of their private lives that profilers possess regardless of how the profilers use the information. Even worse, the information may also be detailed enough to allow holders of the data to engage in identify theft or other financial fraud.

This profiling practice is known as behavioral targeting.[11] The Federal Trade Commission (FTC) recently issued a set of self-regulatory principles to guide advertisers that use behavioral targeting.[12] While compliance is voluntary, these self-regulatory principles are a critical first step toward preventing the harm to consumer privacy that profiling can cause. I will argue, however, that the FTC's principles are inadequate to safeguard consumers' privacy on the Internet.

Part I will explain behavioral targeting, provide some examples of behavioral targeting, and discuss why consumer advocates are justifiably concerned with the possibility that this technology has substantially reduced the privacy of consumers on the Internet. It will also show how (1) profilers' behavioral targeting efforts are often transparent to consumers, thereby creating an information gap that prevents aggrieved consumers from easily redressing any harm that stems from the misuse or inappropriate disclosure of their information, and (2) consumers lack the basic information they need to assess the risk of participating in behavioral targeting. Part I will also describe the compelling benefits of behavioral targeting technology and will argue that these benefits are sufficient that the government should not use regulation to cripple this emerging technology.

Part II will examine the legal framework applicable to companies that engage in behavioral targeting. It will illustrate that (1) no existing law explicitly prohibits behavioral targeting, and (2) that a victim of misuse of their consumer profile will find it difficult to seek redress through either the courts or the FTC. It also will explain how the information gap prevents effective enforcement of applicable law to profilers.

Part III will discuss each of the FTC's recent self-regulatory principles. It will explain why the FTC's approach is a laudable first step because it establishes the standards of care that behavioral marketers must follow. It will also explain why the FTC's approach must be strengthened with oversight and enforcement.

---

11. PRINCIPLES, *supra* note 7, at i-ii.

12. *Id.* at 1-4.

Finally, in Part IV, I will conclude with a survey of others' proposals to strengthen privacy protections related to behavioral targeting. I will also propose FTC enforcement of the self-regulatory principles as mandatory regulations, widening the applicability of the principles' requirements, and a regime of auditing oversight. These proposals would deter misuse of behavioral targeting data, proactively reduce the risk of harm, and give consumers and their advocates the information they need to adequately assess the prevalence of misuse and inappropriate disclosure. The mandatory auditing requirement would ensure that (1) companies engaging in behavioral targeting accurately state how they use consumer information, (2) profilers have appropriate safeguards in place to protect consumer data, and (3) profilers comply with the other requirements of the principles. This proposal seeks to balance consumers' privacy interests and the benefits to consumers and private enterprise that flow from the beneficial use of behavioral targeting.

A variety of consumer advocacy groups and scholars have suggested that even stronger privacy controls on consumer profiling are needed. I will argue, however, that these proposals underestimate the usefulness of behavioral targeting and overestimate the likelihood of otherwise unredressable harm. Several of the stronger controls would ultimately harm consumers by damaging the Internet business models that offer content and services funded or otherwise enabled by behavioral targeting.

I. BEHAVIORAL TARGETING

Behavioral targeting is the use of data about a consumer (a "consumer profile") to provide a service customized for that consumer.[13] Part I provides some examples of how behavioral targeting works on the Internet and then turns to a discussion of the risks and benefits of behavioral targeting.

A. How Behavioral Targeting Works

Because of its prevalence, behavioral advertising–behavioral targeting used for advertising–is at the center of the debate about the privacy implications of compiling consumer preferences.[14] Generally, businesses that use behavioral advertising "track consumers' activities

13. Andrew Hotaling, Comment, *Protecting Personally Identifying Information on the Internet: Notice and Consent in the Age of Behavioral Advertising*, 16 COMMLAW CONSPECTUS 529, 530 (2008), *available at* http://commlaw.cua.edu/res/docs/11_Hotaling.pdf.

14. PRINCIPLES, *supra* note 7, at i-ii.

and associate those activities with a particular computer or device."[15] At present, behavioral advertisers primarily use three approaches to collecting consumers' information: (1) the cookie-based approach, (2) the spyware-based approach, and (3) the deep packet inspection-based approach.[16] Many profilers who employ behavioral targeting for purposes other than advertising also use a fourth approach: the direct collection or "first party" model.

The FTC recently created a simple hypothetical example of how the most common form of behavioral targeting–cookie-based behavioral advertising–works:

> [A] consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights from Washington D.C. to New York City. In this simple example, the travel website where the consumer conducted his research might have an arrangement with a network advertiser to provide advertising to its visitors. The network advertiser places on the consumer's computer a cookie, which is tied to non-personally identifiable information such as the web pages the consumer has visited, the advertisements that the consumer has been shown, and how frequently each advertisement has been shown. Because the newspaper's website is also part of the advertising network, when the consumer visits the newspaper website the network advertiser's cookie identifies the consumer as a visitor to the travel website who likely has an interest in traveling to New York. It then serves the corresponding advertisement for airline flights to New York.
>
> In a slightly more sophisticated example, the information about the consumer's activities on the travel website could be combined with information about the content that the consumer viewed on the newspaper's website. The advertisement served could then be tailored to the consumer's interest in, not just New York City, but also baseball (e.g., an advertisement referring to the New York Yankees).[17]

Cookie-based behavioral advertising relies on cookies to track the consumer. A cookie is a named piece of data that a website sends to a web browser, along with a request that the consumer's web

15. *Id.* at 2.

16. *See infra* Part I.A.

17. *Id.* at 3-4.

browser retain it.[18] The website can indicate how long the web browser should retain the cookie, and for which website or websites the data in the cookie is intended.[19] Then, each time the consumer uses the web browser to visit the corresponding website or websites, the consumer's web browser sends the content of the cookie back to the website.[20] By assigning each web browser a cookie with a unique number, a behavioral advertiser's website can later differentiate and profile the activities of the many consumers using the website.[21]

Many businesses that use this form of behavioral advertising take advantage of the services of "network advertisers."[22] Network advertisers are "companies that select and deliver advertisements across the Internet at websites that participate in their networks."[23] These ads are targeted using profiles that describe the consumer's activities at *all* of the sites within the advertising network.[24] This network can "include hundreds or thousands of different, unrelated websites."[25] Thus, the network advertiser can compile a rich profile about the activities of consumers using each computer or device.[26]

Network advertisers use cookies in a sophisticated way to track consumer behavior.[27] First, they solicit websites to become part of their advertising networks.[28] Then, when a consumer first visits a website that is a member of an advertising network, the member website sends a cookie with a unique tracking number to the web browser.[29] This cookie is configured to be included with all requests

---

18. DINO ESPOSITO, PROGRAMMING MICROSOFT ASP.NET 2.0 538 (Microsoft Press 2006).

19. Msdn.microsoft.com, HTTP Cookies, http://msdn.microsoft.com/en-us/library/aa384321(VS.85).aspx (last visited May 10, 2009).

20. *See id.*

21. *See, e.g.*, Katherine McKinley, Cleaning Up After Cookies Version 1.0, at 1, 2 (Dec. 31, 2008), https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf (noting that websites use browser-based plug-ins to store information used for "credentials (username/passwords and equivalents), tracking users, storing preferences (interface customizations, volume controls), site data (security questions, images, cached data), identifying tokens, or other data").

22. PRINCIPLES, *supra* note 7, at 2-3.

23. *Id.* at 3.

24. *Id.* at 3 n.5.

25. *Id.*

26. *Id.* at 2-3. Moreover, "an individual website may belong to multiple networks." *Id.* at 3 n.5.

27. PRINCIPLES, *supra* note 7, at 2.

28. *Id.* at 2-3.

29. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001).

for content sent to any of the network advertiser's member websites.[30] Thus, each time the consumer visits any of the member websites, the network advertiser can associate the consumer with the web content that the consumer accessed.[31]

Typically, some placeholder content element on the requested web page from the member's website–typically a banner image or a "box"–will direct the consumer's web browser to the network advertiser's website.[32] The consumer's web browser then dutifully loads a targeted advertisement from the network advertiser's website into the placeholder banner image or "box."[33] When the consumer's web browser requests this content from the network advertiser's website, the web browser includes the cookie containing the unique tracking number as part of the request.[34] The request also contains data indicating the webpage on the member's website that the user had requested.[35] This allows the network advertiser to track the consumer's activities across multiple websites in the advertiser's member network[36] and pay member websites when they supply consumers to the network advertiser.[37] This behavior is hidden from the consumer; the consumer does not normally know anything about the cookies, which websites are members of which advertisers' networks, or what information a member website might share with the network advertiser.[38]

Generally, the data that behavioral advertisers collect is not personally identifying because it does not include the consumer's name, physical address, or other personal identifiers that could translate directly to the "offline world."[39] Unless a consumer discloses her name or other personally identifying information to a website that is a member of the behavioral advertiser's member network, the behavioral advertiser only knows the consumer by a unique

30. *Id.*

31. FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 2-6 (2000) [hereinafter REPORT TO CONGRESS], *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf.

32. *Id.* at 3, n.1 (referring to beacons as "web bugs"); *DoubleClick*, 154 F. Supp. 2d at 503.

33. *See DoubleClick*, 154 F. Supp. 2d at 503 (referring to the "boxes" as "blank spaces").

34. *Id.*

35. *Id.*

36. *See id.* at 503-505.

37. Google, AdSense, https://www.google.com/adsense/login/en_US/ (last visited Mar. 28, 2010).

38. *DoubleClick*, 154 F. Supp. 2d. at 504.

39. *Id.* at 502.

identifying number in the cookie.[40] Even so, because a behavioral advertiser's profile of a consumer becomes more detailed through the accretion of data from many websites over time, the detail makes it correspondingly easier to identify the profiled consumer.[41]

Because of their role in enabling this process, some consumers have become critical of cookies, and their concerns have led developers of web browsers to create features to aid consumers in managing and blocking cookies.[42] Indeed, a consumer might effectively opt out of all behavioral profiling if the consumer either configured his web browser to refuse to accept cookies, or constantly removed all cookies from the web browser's memory.[43] A consumer's antivirus software could also conceivably thwart behavioral advertisers if it watched for and deleted cookies known to be associated with a behavioral advertiser's web servers.[44]

Usually, however, because cookies are so critical to website development, disabling or blocking them tends to cause errors and can result in an unsatisfactory experience with many websites.[45]

---

40. *DoubleClick*, 154 F. Supp. 2d at 503.

41. Barbaro & Zeller, *supra* note 1.

42. *See, e.g.*, Microsoft Support, The Default Privacy Settings for Internet Explorer 6, http://support.microsoft.com/kb/293222/EN-US/ (last visited July 24, 2010) (noting the creation of a new "Privacy tab" in Internet Explorer 6 to allow users to configure cookie settings); Google Chrome, Cookies: Manage Cookies, http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95647 (last visited July 24, 2010) (explaining how and why to use Google Chrome's cookie-blocking features); Complaint at 15, Valentine v. NebuAd, No. CV 08 5113, (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ ("As software programs that filtered online activity and deleted browser cookies developed[,] . . . the consumer gained control over . . . attempts at data collection.").

43. *See* ESPOSITO, *supra* note 18 ("The downside of cookies is . . . the fact that the user can disable them."); *see also DoubleClick*, 154 F. Supp. 2d at 504-05 (noting that a user may opt out of DoubleClick's behavioral advertising regime by configuring their browser to block cookies).

44. *See* Cristina Mailat, *Tracking Cookies and How to Delete Them,* IDSECURITYSUITE, Dec. 18, 2007, http://www.idsecuritysuite.com/blog/tracking-cookies-and-how-to-delete-them.

45. *See* HTTP Cookies, *supra* note 19 (noting the usefulness of the cookies to website developers). Google's new Chrome web browser takes a different approach with its "incognito" mode: it accepts cookies, but deletes them at the end of the browsing session. Google Chrome, Explore Google Chrome features: Incognito Mode, http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464 (last visited May 10, 2009). This approach may deliver a better user experience while still improving privacy because the cookie mechanism still works, but any tracking cookies would be automatically deleted at the end of the session. *See id.* But, Chrome itself may be criticized for sending too much information to Google. Google Chrome, Google Chrome Privacy Notice, http://www.google.com/chrome/intl/en/privacy.html (last visited May 10, 2009) (noting that Chrome sends Google a list of visited website and queries).

Indeed, website developers often must use cookies to identify a web browser between requests for web pages because the hypertext transfer protocol, which describes the rules computers follow when they load web pages, is "stateless."[46] This means that if a website developer wants to create a process that remembers the consumer's identity across visits to multiple web pages (the procedure of adding items to an online shopping cart is the paradigmatic example of this), the website developer must use cookies (or some other means) to distinguish the consumer from other consumers and remember the context of that consumer's earlier visits.[47] In the shopping cart example, for instance, the website must be able to identify the consumer so that it can check its memory to see which items are in the associated consumer's shopping cart and where the associated consumer is in the checkout process.[48]

The two other methods that behavioral advertisers already commonly use to track consumers on the Internet do not rely on cookies.[49] Both methods are relatively more subtle, unexpected, and difficult for the consumer to detect or avoid.[50]

First, a consumer's ISP or a website the consumer visits can install software directly to the consumer's computer to view data that the computer exchanges with other computers on the Internet.[51] Potentially, such a profiler could observe the consumer's entire stream of Internet traffic–*all* data that the consumer's computer sends or receives.[52] This software might fairly be characterized as spyware.[53]

Before installation, a consumer might know only that a website he or she visited wanted to install software to his or her computer and believe that the software was needed to display a desired website–perhaps even the ISP's own website.[54] Or, he or she might wish to

---

46. *See* ESPOSITO, *supra* note 18, at 538.

47. *See* Cookiecentral.com, Cookies and Privacy FAQ, http://www.cookiecentral.com/n_cookie_faq.htm (last visited May 10, 2009).

48. *See id.*

49. *See infra* Part I.A.

50. *See infra* Part I.A.

51. Chloe Albanesius, *Should Your ISP be allowed to Serve You Spyware?,* PC MAGAZINE, Apr. 28, 2008, http://www.pcmag.com/print_article2/0,1217,a=226952,00.asp?hidPrint=true.

52. *Id.*

53. *See id.* The author of the article describes this software as spyware. This is probably a fair characterization of what the software does, but producers of this software would undoubtedly resist this characterization.

54. *See id.* (noting that, according to the Anti-Spyware Coalition, ISPs may "partner with

download the software to get some benefit the program offers without knowing that the program also tracks Internet use.[55] For instance, Google's Chrome web browser, while probably not popularly considered spyware, discloses to Google all of the searches and URLs entered into the address bar.[56]

Once installed, the software can operate transparently and, thus, only the most vigilant consumers (perhaps equipped with anti-spyware software) would learn that they were being tracked.[57] Even then, it might be difficult for the consumer to know where the tracking software originated, and it may be impossible to know which profiler was doing the tracking or what information the profiler obtained.[58]

On the other hand, the software could also be written to disclose its existence, purpose, and activities to the computer user.[59] Some consumers might be willing to allow a profiler access to this information in exchange for a targeted service.

The final common method of behavioral advertising, deep packet inspection (DPI), is even more subtle and difficult to detect, because this method gives the consumer no indication that her activities are being tracked.[60] Using this approach, the consumer's ISP (or a partner company)[61] installs powerful hardware devices[62] that examine all of

---

targeting companies in order to give access to a user's entire traffic stream with little or notice and consent").

55. *See* Google Chrome, Google Chrome Privacy Notice, http://www.google.com/chrome/intl/en/privacy.html (last visited May 10, 2009) (noting that Chrome sends Google a list of visited website and queries).

56. *Id.* To be fair, Chrome has to supply Google with the text of searches so that Google can perform the search and return the results to the consumer's web browser. Nevertheless, Google has no similar functional need to know the address of every website a consumer visits.

57. CTR. FOR DEMOCRACY & TECH., ANTI-SPYWARE COALITION DEFINITIONS DOCUMENT, WORKING REPORT, Nov. 12, 2007, http://www.antispywarecoalition.org/documents/documents/2007definitions.pdf (last visited April 6, 2009).

58. *Id.*

59. *Id.* at 2.

60. *See* Complaint at 17, 21, Valentine v. NebuAd, No. CV 08 5113, (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ (alleging that ISPs allowed NebuAd to "tap[] directly into the consumer's ISP connection").

61. *See id.* at 17.

62. *See What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies Before the H. Comm. on Energy and Commerce, Subcomm. on Telecommunications and the Internet,* 110th Cong. 2 (2008) [hereinafter *Statement*] (statement of Alissa Cooper, Chief Computer Scientist, Center for Democracy & Technology), *available at* http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-

the Internet traffic going to or originating from consumers' computers.[63] While there could be a variety of uses for this data, one possible use is to compile information of interest to marketers.[64] Indeed, an ISP could sell this information to marketers to create additional revenue.[65] The DPI method does not require any software to be installed on the consumer's computer, nor would an anti-spyware program be able to easily detect it.[66]

Further, this method of profiling is practically impossible to stop or avoid.[67] While consumers can remove tracking cookies and spyware from their computers to protect their privacy from the previously described methods of tracking, there is little that they can do to protect themselves from DPI-based profiling.[68] The only limiting factor is that the required network hardware would need to be within the ISP's traffic "stream," so this method would require the cooperation of the ISP.[69] The *Washington Post* estimates that "at least 100,000 U.S. customers are tracked this way," and that ISPs "have

---

ti-hrg.071708.Cooper-testimony.pdf (noting the computational power to perform this kind of inspection has only recently become available). Ordinarily, internet routers examine only the headers of packets of data. This header information is analogous to the address information on an envelope of postal mail. This necessary practice is known as shallow packet inspection. During shallow packet inspection, the router needs only to examine a small portion of the data and only for the purpose of deciding where to send the data. By comparison, deep packet inspection devices are capable of not only reading the information on the outside of the envelope but the letter inside during the course of delivery. *Id.* at 2, 4-6.

63. Peter Whoriskey, *Every Click You Make: Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising*, WASH. POST, Apr. 4, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html. By contrast, with the conventional cookie-based approach, the behavioral marketer can learn only whatever a user communicates to websites that are part of the marketer's network of websites. PRINCIPLES, *supra* note 7, at 16, n.40. However, at present, deep packet inspection cannot inspect encrypted packets, which are commonly exchanged when a user supplies sensitive financial data like credit card numbers. *Statement, supra* note 62, at 5.

64. Whoriskey, *supra* note 63.

65. *Id.*

66. *Id.*

67. *See* Complaint at 15, 22, Valentine v. NebuAd, No. CV 08 5113, (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ (noting that consumers used a variety of methods to control profilers' data collection efforts); *Statement, supra* note 62, at 3 (noting that "existing opt-outs merely discontinue the creation of behavior profiles" rather than terminating the inspection of the consumer's internet traffic); *id.* at 12-13 (noting that only the "most sophisticated and technically savvy consumers are likely to be able to successfully negotiate such opt-out processes").

68. *See Statement, supra* note 62, at 15 (alleging that consumers used these methods to control the disclosure of their information).

69. *Id.* at 6.

been testing it with as many as 10 percent of U.S. customers."[70] As with the other approaches, it may be impossible–or at least very difficult–to know what information a marketer collects using this method.[71] And, while some DPI providers may have a mechanism for allowing users who are aware of the DPI to opt out of the profiling, this opt-out may stop only the storage of consumer information, rather than the DPI itself.[72] Some ISPs, perhaps fearing a negative customer reaction, are expressly and publicly disavowing any use of this technology within their own networks, and indicating their belief that this kind of profiling should only take place with the customer's consent.[73]

The data that a profiler gleans using either of these two latter methods could be used to select and display an appropriate advertisement.[74] If, however, the profiler also possesses the necessary names, addresses, e-mail addresses, or telephone numbers, the profiler may be able to combine the data for direct mail and e-mail marketing campaigns, telephone marketing, or any other form of behavioral advertising.[75] Since ISPs and some other service providers must retain consumers' information for billing purposes, the potential for combining a consumer's behavioral profile with billing information is a concern, particularly since the consumer likely expects billing information to be used solely for billing purposes.[76]

Indeed, all of the foregoing forms of behavioral targeting are invisible to the consumer[77] unless the profiler discloses the profiling.[78] Profilers may even be taking advantage of their obscurity

---

70. Whoriskey, *supra* note 63.

71. *See* Complaint at 17-18, Valentine v. NebuAd, No. CV 08 5113, (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ (noting that NebuAd, in its patent application claimed that its deep packet inspection device would be transparent to the user).

72. *Statement, supra* note 62, at 3.

73. *See* Roy Mark, *Broadband Providers Vow to Protect User Privacy*, EWEEK.COM, Sep. 26, 2008, *available at* http://www.eweek.com/c/a/Enterprise-Applications/Broadband-Providers-Vow-to-Protect-User-Privacy/.

74. *Statement, supra* note 62, at 6-7.

75. *See* PRINCIPLES, *supra* note 7, at 22 ("[D]epending on the way information is collected and stored, it may be possible to link or merge non-PII with PII. For example, a website might collect anonymous tracking data and then link that data with PII (e.g., name, address) that the consumer provided when registering at the site.").

76. *See id.*

77. Hotaling, *supra* note 13, at 548, 558.

78. A recent article in the *New York Times* alluded to consumers' hopelessness when it comes to truly understanding the privacy implications of their actions:

> Enter the post-privacy society, where we have lost track of how many entities are

to sidestep the negative consumer sentiment that would result if consumers had to be explicitly told when profilers were collecting information about them and their Internet activities.[79]

Profilers certainly benefit from their obscurity when it comes to avoiding liability for inappropriate disclosure. Even if a consumer suspected that the contents of his profile had been inappropriately used or disclosed, it would be difficult for him to discern which profiler was at fault, and, therefore, which company to contact or, perhaps, to sue.[80] Because consumers lack this information, they may be without effective legal recourse when a profiler's use of behavioral targeting harms them.[81]

Perversely, this situation also leaves profilers with little incentive to improve their privacy protections.[82] Presumably, because consumers lack the basic information they would need to hold profilers accountable when they improperly disclose consumer data, consumers and consumers' agents (like banks that provide protections from identity theft and financial fraud) are left to bear the costs of the improper disclosure.[83] Thus, the transparency of behavioral targeting creates a formidable information gap between consumers on one hand and profilers on the other. This gap is a significant obstacle to assessing the prevalence of these risks and to holding profilers accountable when misuse occurs.

The final method of profiling is far more explicit to consumers. This method, which the FTC refers to as "first party" targeting, "involves targeting based on data collected at and by a single website."[84] The FTC views this method of profiling as relatively

---

> tracking us. Not to mention what they are doing with our personal information, how they are storing it, whom they might be selling our dossiers to and, yes, how much money they are making from them. On the way out, consumer advocates say, is that quaint old notion of informed consent, in which a company clearly notifies you of its policies and gives you the choice of whether to opt in (rather than having you opt out once you discover your behavior is being tracked). "How does notice and choice work when you don't even interface with the company that has your data?" says Jessica Rich, a deputy director of the bureau of consumer protection at the Federal Trade Commission.

Natasha Singer, *Shoppers Who Can't Have Secrets*, N.Y. TIMES, May 2, 2010, at BU5, *available at* http://www.nytimes.com/2010/05/02/business/02stream.html.

79. Hotaling, *supra* note 13, at 559. It is indeed ironic that consumers have so little privacy from profilers, but profilers have almost complete privacy from consumers!

80. *Id.*

81. *Id.*

82. *Id.*

83. *See id.*

84. PRINCIPLES, *supra* note 7, at 26.

innocuous because it is "more likely to be consistent with consumer expectations, and less likely to lead to consumer harm" when compared to profiling "involving the sharing of data with third parties or across multiple websites:"[85]

> [G]iven the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.[86]

The FTC concluded that "first party" targeting did not pose as much risk "that the data will fall into the wrong hands" compared to the other methods of profiling, and that, therefore, its self-regulatory principles would not apply to first party targeting.[87]

For instance, Netflix, an Internet-based movie rental service, aggregates information about consumers' preferences to suggest movies that subscribers are likely to enjoy.[88] Since Netflix uses this information to target suggestions to existing subscribers,[89] it is not advertising in the traditional sense, even though Netflix uses this capability to encourage a service subscriber to maintain or increase the subscriber's use of the service.[90] Similarly, Facebook collects biographical information from each subscriber to suggest people the subscriber might know because they have mutual friends, because they worked in the same place, or because they attended the same school.[91]

---

85. *Id.*

86. *Id.* at 27.

87. *Id.* at 27.

88. Clive Thompson, *If You Liked This, You're Sure to Love That*, N.Y. TIMES, Nov. 23, 2008, (Magazine), at MM74, *available at* http://www.nytimes.com/2008/11/23/magazine/23Netflix-t.html.

89. *Id.*

90. *See id.*

91. Florin Ratiu, *People You May Know*, *The Facebook Blog*, FACEBOOK, http://blog.facebook.com/blog.php?post=15610312130. Of course, Facebook also is known for using customers' profiles for targeted advertisements as well. Facebook, Facebook Advertising,

Services like Netflix and Facebook are exciting and useful because they aggregate information about consumers to deliver a valuable product that would not be possible otherwise.[92] Indeed, while behavioral advertising is sometimes used as a synonym for behavioral targeting,[93] behavioral advertising should be understood as the use of behavioral targeting for advertising purposes.[94] Some applications of behavioral targeting, like the services offered by Netflix and Facebook, have only a strained connection to advertising in the traditional sense. These applications of behavioral targeting enable Internet businesses to deliver services that simply would not have been possible without the use of consumer profiles. Nonetheless, these technologies still must collect data about consumers to be effective,[95] and therefore present the same privacy concerns as are inherent in any behavioral targeting endeavor.

B. The Risks of Behavioral Targeting

Consumer and privacy advocates are concerned that the compilation of extensive profiles containing information about consumers and their behavior can harm consumers.[96] This subsection explains how behavioral targeting can harm consumers and the circumstances when these harms can occur. It also explains how consumers are in a poor position to effectively manage the risks associated with profiling. Finally, it discusses profilers' attempts to manage these risks through anonymization.

1. How Behavioral Targeting Harms Consumers

Behavioral targeting is not a new phenomenon, nor does it occur solely on the Internet. Indeed, in 1999, the FTC became interested in

---

http://www.facebook.com/advertising/ (last visited Mar. 28, 2010); Duncan Riley, *Facebook Will Use Profiles to Target Ads, Predict Future*, TECHCRUNCH, Aug. 22, 2007, http://techcrunch.com/2007/08/22/facebook-will-use-profiles-to-target-ads-predict-future/; Vauhini Vara, *Facebook Gets Personal With Ad Targeting Plan*, WALL ST. J., Aug. 23, 2007, at B1, *available at* http://online.wsj.com/article/SB118783296519606151.html?mod=rss_whats_news_technology.

92. LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY 122-141 (2008).

93. *See, e.g.*, Letter from Privacy Advocates to Donald S. Clark, Secretary, Fed. Trade Comm'n, at 6 [hereinafter Privacy Letter], *available at* http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

94. *See infra* Part III (observing that the FTC makes a similar distinction in the scope of its new self-regulatory principles).

95. *See id.*

96. PRINCIPLES, *supra* note 7, at i-ii.

the risks associated with behavioral targeting when DoubleClick, a company specializing in Internet-based behavioral advertising, purchased Abacus Direct, a direct marketing services corporation maintaining information on American customers' "offline" retail habits.[97] The FTC worried that DoubleClick would be able to combine its Internet consumer database with the purchased Abacus database describing consumer's "offline" habits[98] and that the combination would sharply increase the detail with which the merged organization would be able to view the consumers it had profiled.[99]

After investigating, the FTC concluded that its fears were unfounded because DoubleClick had not combined its Internet-based database with Abacus' "offline" database.[100] Nevertheless, the proliferation of behavioral targeting makes it likely that Internet profiling will become so much more extensive and thorough that Internet profiles will grow to contain as much detail as a combined DoubleClick database would have, even though the Internet profile is never merged with a source of "offline" information.

Nevertheless, as this part shows, the existence of these consumer profiles, replete with information about the consumer and his or her habits, puts all consumers in danger of (1) losing the ability to shield intimate and personal details of their private lives from the view of profilers who wish to use this data as a marketing tool, (2) embarrassment from the unexpected disclosure of details about a consumer that a consumer expected to remain private, (3) identity theft or other forms of financial fraud made possible by the richness of detailed information present in a consumer's profile, and even (4) the unexpected use of a consumer's profile to make adverse decisions about how to treat her.

First, consumer and privacy advocates criticize behavioral targeting because it results in the compilation of a sizable array of potentially sensitive data about the consumer that exists outside her ability to protect, control, or monitor.[101] Indeed, profiling arguably

97. *DoubleClick,* 154 F. Supp. 2d at 505.

98. *Id.*

99. *See id.* (noting that the combination could "create a super-database capable of matching [consumers'] online activities with their names and addresses"); *see also* Complaint and Request for Injunction, Request for Investigation and for Other Relief at 6-10, In the Matter of DoubleClick, before the Fed. Trade Comm'n (Feb. 10, 2000), *available at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf (noting that a combined database would violate consumers' expectations of privacy and alleging that it constitutes an unfair practice under the FTC Act).

100. *In re* DoubleClick, 154 F. Supp. 2d at 506.

101. *Cf.* Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal*

harms consumers regardless of how it is used because it results in an unprecedented loss of privacy. By merely participating in the Internet economy, consumers lose control over which details about their private lives are known,[102] and they have little control over who gets to learn of these details after the data passes into a profiler's hands.[103] Nor do consumers have any control over the way a profiler mines compiled data to construct a "picture" of an individual consumer, even though this data mining can generate a far more intrusive "picture" of the consumer's life than he might expect.[104] In creating this picture, the profiler learns and potentially communicates something private about the consumer that he has not authorized the profiler to know.[105]

Secondly, sometimes this unauthorized picture can be embarrassing, regardless of whether it is disclosed inadvertently or intentionally.[106] This embarrassment is itself a type of harm that the law has been willing to remedy in other contexts.[107]

Even worse, in the wrong hands, a consumer's profile could facilitate financial fraud or identity theft.[108] Thus, a consumer whose

---

Identifying Information Through Enhanced Privacy Policies and Laws, 19 ALB. L.J. SCI. & TECH. 91, 93 (2009) (discussing how consumers lose control over personally identifying information (PII) when they disclose it to businesses, and how businesses use PII for data mining).

102. *Id.* at 93; *see also id.* at 111 (discussing the embarrassment inherent in a physician permitting an "unmarried man with no medical training to be present when a woman gave birth").

103. *Id.* at 93.

104. *Id.* at 95-96.

105. *See id.* Some behavior advertisers do not believe that consumers should have a right of privacy in these details. PRINCIPLES, *supra* note 7, at 31 ("These commenters suggested that consumers do not own the data that websites collect about them, and that there is no precedent for giving consumers the ability to dictate the terms upon which they use a website."). *See also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 199 (1890), *available at* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html ("[T]he individual is entitled to *decide whether that which is his shall be given to the public.* No other has the right to publish his productions in any form, without his consent.") (emphasis added).

106. *See* Barbaro & Zeller, *supra* note 1.

107. Warren & Brandeis, *supra* note 105, at 197. ("[M]odern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."). Warren and Brandeis, however, premised their influential ideas about privacy on the problem of gossipy newspapers. JOHN L. DIAMOND, ET. AL, UNDERSTANDING TORTS 387, n.2 (3rd. ed. 2007). Because the social value of gossip is low, it was comparatively easy for courts to follow the Warren and Brandeis article into recognizing a right to privacy. However, with behavioral targeting's comparatively substantial benefits to consumers and society, it is more difficult to make a plausible case that consumers have an absolute right to privacy or complete control of their data. *See infra* part II.C.

108. *See* Sprague & Ciocchetti, *supra* note 101, at 101-02 (describing the risks of identity

data is inappropriately disclosed might experience harm because she must take steps to prevent, monitor, or remedy identity theft or other financial fraud.[109]

Finally, consumer and privacy advocates also fear that the use of behavioral profiles to make decisions that may be inappropriate (or at least surprising) uses of consumer data.[110] For instance, insurers or potential creditors might wish to use a consumer's profile in an attempt to establish pricing for their products.[111] In addition, Internet retailers may use consumer data to engage in a practice of differential pricing for consumers based on a behavioral profile.[112]

2. The Mechanisms of Inappropriate Disclosure

When a profile paints an intrusive picture of a consumer, the collection of the profile itself may harm the consumer regardless of how the profile is used. But some other harms that consumer and privacy advocates anticipate are contingent on the inappropriate use

---

theft and financial fraud inherent with the disclosure of personally identifying information (PII)). While the profiles that result from behavioral targeting may not contain PII, the aggregation of even non-personally identifying information ultimately forms such a complete picture of a consumer as to pose the same risks. *See* Barbaro & Zeller, *supra* note 1.

109. *E.g.*, Sandy Kleffman, *Kaiser Warns Nearly 30,000 Employees of Data Breach,* SAN JOSE MERCURY NEWS, Feb. 6, 2009, http://www.mercurynews.com/ci_11646163?nclick_check=1 (last visited Apr. 19, 2009) (describing how a Kaiser Permanente data breach is believed to have resulted in identity theft for several Kaiser Permanente employees whose data was described in the data lost in the breach). *See also* Federal Trade Commission, *Defend: Recover From Identity Theft, Fighting Back Against Identity Theft,* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html (last visited Apr. 19, 2009) (describing the many steps an identity theft must go through to minimize the effects of the crime). *But see* Sasha Romanosky, et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?, Seventh Workshop on the Economics of Information Security,* June 25-28, 2008, http://weis2008.econinfosec.org/papers/Romanosky.pdf (" The probability of becoming a victim to identity theft as a result of a data breach is very low, around only 2%."). Even if true, this observation confirms that there is a measurable positive correlation between identity theft and data breach. Nevertheless, it can be difficult to confirm whether incidents of identity theft are attributable to a particular data breach. *See* Randy Ludlow & Holly Zacariah, *Hacked Off: Data Thefts Leave Ohio University Scrambling, Students and Alumni Steaming,* COLUMBUS DISPATCH, Jun. 19, 2006, at 1A (noting that although officials were not aware of any confirmed cases of identity theft related to a data breach, 24 cases of identity theft were under investigation).

110. Center for Democracy and Technology, *Privacy Impact, Guide to Behavioral Advertising,* Oct. 27, 2009, http://www.cdt.org/content/privacy-impact (last visited Mar. 28, 2010) [hereinafter *Privacy Impact*].

111. *Id.* ("Behavioral profiles, particularly those that can be tied to an identifiable individual, may also be a tempting source of information for companies making decisions about people's credit, insurance or employment.").

112. *Id.*

or disclosure of consumer data. Understanding how inappropriate use or disclosure occurs, therefore, is a predicate to discussing the appropriate legislative or regulatory methods of preventing these harms.

First, ample anecdotal evidence shows that corporations and other consumer information profilers have difficulty securing their data.[113] There are a variety of overlapping threats. Corporations occasionally lose and misplace backup tapes[114] and other archival media.[115] They lose data when laptops (and, increasingly, also mobile devices like Blackberries[116]) containing sensitive data are lost or stolen.[117] Corporations occasionally lose data because hackers or malware penetrate their electronic defenses.[118] Sometimes they lose

---

113. *See generally* Sprague & Ciocchetti, *supra* note 101, at 97-101.

114. *E.g.*, Jon Oltsik, *Perspective: One Less Data Breach Method to Fret About*, CNET NEWS, Feb. 7, 2006, http://news.cnet.com/One-less-data-breach-method-to-fret-about/2010-1029_3-6035850.html (last visited April 13, 2009) (describing data breaches at Bank of America, Citibank, Marriott, and Time Warner); Ingrid Marson, *Marriott Loses Data on 200,000 Customers*, CNET NEWS, Jan. 3, 2006, http://news.cnet.com/Marriott-loses-data-on-200,000-customers/2100-1029_3-6015768.html (describing data breach at Marriott); Dawn Kawamoto, *Data for 600,000 Time Warner Employees MIA*, CNET NEWS, May 2, 2005, http://news.cnet.com/Data-for-600,000-Time-Warner-employees-MIA/2100-1029_3-5692534.html (describing loss of Time Warner backup tapes during transport to storage facility).

115. *E.g.*, Leo King, *Virgin Media Loses Unencrypted CD With 3,000 Customer Bank Details*, COMPUTERWORLD UK, June 23, 2008, http://www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=9687 (describing how Virgin Media lost a CD containing unencrypted customer banking details in spite of a company policy prohibiting this data from being transmitted without encryption).

116. *E.g.*, *Cabinet Data on Stolen BlackBerry*, BBC NEWS, Apr. 11, 2009, http://news.bbc.co.uk/1/hi/uk/7994850.stm (last visited Apr. 13, 2009), *available at* http://news.bbc.co.uk/2/hi/uk_news/7994850.stm; Yuki Noguchi, *Lost a BlackBerry? Data Could Open A Security Breach*, WASH. POST, Jul. 25, 2005, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html.

117. *E.g.*, Robert McMillan , *Boeing Laptop Theft Puts U.S. Data Breach Tally Over 100M; A Privacy Group Has Kept Tabs on Incidents Since February 2005*, COMPUTERWORLD, Dec. 15, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006140 (discussing data breaches associated with lost laptops at Boeing); Nathan McFeters, *Stanford University Data Breach Leaks Sensitive Information of Approximately 62,000 Employees*, ZERO DAY, June 23, 2008, http://blogs.zdnet.com/security/?p=1326.

118. *E.g.*, Joel Hruska, *Malware Infestation Responsible for Credit Card Data Breach*, ARS TECHNICA, Jan. 20, 2009, http://arstechnica.com/security/news/2009/01/malware-infestation-responsible-for-credit-card-data-breach.ars (describing a credit card data breach at a major processing company stemming from a malware infection and indicating the company does not plan to provide credit monitoring to affected persons because the company concluded the data breach did not pose this risk to consumers); Kim Zetter, *Card Processor Admits to Large Data Breach*, WIRED.COM, Jan. 20, 2009, http://blog.wired.com/27bstroke6/2009/01/card-processor.html (describing the same data breach

data to disgruntled employees.[119] Other times, data is lost because of bugs in Internet-enabled software.[120] This loss happens in spite of laws requiring these profilers to undergo expensive notification campaigns when they have such disclosure.[121] Some of these breaches might be a result of a profiler's negligent safeguards, but, in other cases, profilers are victims of others' malfeasance in spite of instituting safeguards. Moreover, everyone must wonder how many data losses go undetected and unreported.[122]

In addition to losing data describing their customers, profilers often share the data they collect about consumers. Companies commonly share a customer's information across their business units, and, of course, with contractors the company employs to provide its products or services.[123] Some companies sell valuable data to

---

as the result of hacking); Brian Krebs, *Justice Breyer Is Among Victims in Data Breach Caused by File Sharing*, WASH. POST, July 9, 2008, at A01 (describing data breaches resulting from employee use of peer-to-peer file sharing programs). The distinction between malware and hacking is, perhaps, misleading. Hackers often use malware as the instrumentality of their fraud. *See* Zetter, *supra* note 118. Data breaches are not unique to corporations. "Higher education is a juicy target [for hackers] because it compiles so much personal information in so many places." Ludlow and Zacariah, *supra* note 109.

119. *E.g.*, Brian Krebs, *Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People*, WASH. POST, Jan. 6, 2009, at D02 (noting "the percentage of breaches attributed to data theft from current and former employees more than doubled from 7 percent in 2007 to nearly 16 percent in 2008.").

120. Jason Kincaid, *Google Privacy Blunder Shares Your Docs Without Permission*, TECHCRUNCH, Mar. 7, 2009, http://www.techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/ (describing a problem in Google Docs that inadvertently allowed former collaborators to access documents the owner had revoked access to); Jenna Wortham, *Facebook Glitch Brings New Privacy Worries*, N.Y. TIMES, May 6, 2010, at B1. This sort of problem can be expected to become even more common as rapidly developed software becomes more common. This software development approach speeds the release of new features to users, but at the "cost" of rigorous testing. Or, perhaps a better way to put it is that the earliest users perform the testing that software testers might have done.

121. *E.g.*, Brian Krebs, *Data Breaches Are More Costly Than Ever*, WASH. POST, Feb. 3, 2009, at D03 (according to a new study, "[o]rganizations that experienced a data breach in 2008 paid an average of $6.6 million last year to rebuild their brand image and retain customers . . . ."); CAL. CIV. CODE §§ 1798.29, 1798.82, and 1798.84 (West 2008); COLO. REV. STAT. § 6-1-716 (2008); Sprague & Ciocchetti, *supra* note 101, at 101-02. Note that, while data breach laws are common, most do not require the breached entity to do anything more than notify consumers of the breach. *Id.* at 102.

122. *See, e.g.*, Thomas Claburn, *Most Security Breaches Go Unreported*, INFORMATION WEEK, Aug. 1, 2008, http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=209901208 (noting that according to one survey, "[m]ore than 89% of security incidents went unreported in 2007.").

123. DANIEL SOLOVE ET AL., INFORMATION PRIVACY LAW 623 (2d ed. 2006); Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled With Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 29-30 (2008).

"partners" that use the data for marketing purposes not connected to the original company's business units.[124]

Profilers may also be required to share the data they collect with law enforcement authorities and litigants.[125] Indeed, a person's right to privacy relative to government agents in this context is much weaker than consumers probably expect.[126] An individual's right to privacy in any information that a third party holds is extremely limited.[127] Many profilers include warnings in their privacy statements that a consumer's profile may have to be disclosed to law enforcement authorities.[128] And, this data may occasionally be at risk because it could be discoverable in civil litigation.[129]

3. The Role of the Consumer

Consumers are in poor positions to protect themselves from these harms. They lack the information that they need to make rational decisions about whether to participate in activities on the Internet that involve behavioral targeting.

The fundamental calculus of risk aversion is a familiar tort

---

124. SOLOVE, *supra* note 123, at 623; Ciocchetti, *supra* note 123, at 18.

125. *See infra* notes 128-131.

126. *See* United States v. Miller, 425 U.S. 435, 442-44 (1976) (concluding a person has no reasonable expectation of privacy in his bank's imaged check records, even though that consumer gives data to the bank for a limited purpose, because when a person gives information to a third party, the person takes the risk that the third party will disclose the data to the government); California v. Greenwood, 486 U.S. 35, 40-41 (1988) (concluding a person has no expectation of privacy in trash placed for collection outside the home, even though it may reveal intimate details of the private behavior going on inside the house, because when left in public, the trash is accessible to animals, children, and others). When a person has no reasonable expectation of privacy in a certain piece of information, the legal result is that government agents need neither a warrant nor probable cause to obtain the information. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (confirming that Fourth Amendment protections can attach only when a person has a reasonable expectation of privacy). *See generally* Sprague & Ciocchetti, *supra* note 101, at 114-16.

127. Sprague & Ciocchetti, *supra* note 101, at 116 (surveying cases and concluding that individuals have no right to privacy in the "'to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account'" or "'subscriber information provided to an internet provider'"); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).

128. *E.g.*, Facebook, Privacy Policy, http://www.facebook.com/policy.php?ref=pf (last visited Apr. 19, 2009) ("We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."); Netflix, Privacy Policy, http://www.netflix.com/PrivacyPolicy (last visited Apr. 19, 2009) ("Netflix also reserves the right to disclose personal information when we reasonably believe disclosure is required by law, if we reasonably believe disclosure is necessary to establish or exercise legal rights, or in situations involving potential threats to physical safety.").

129. *Privacy Impact*, *supra* note 110.

concept to most lawyers. As Judge Learned Hand wrote:

> The degree of care demanded of a person by an occasion is the resultant of three factors: the likelihood that his conduct will injure others, taken with the seriousness of the injury if it happens, and balanced against the interest which he must sacrifice to avoid the risk.[130]

Judge Hand later expressed this analysis in a formula:

> [I]f the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e. whether B < PL.[131]

In short, under Judge Hand's intuitive analysis, a person is negligent in taking precautions to avoid a particular harm when the person refuses to incur a precautionary cost or burden that is less than the magnitude of the loss multiplied by the probability of the loss.[132]

Judge Hand's calculation is readily adaptable to the analysis that consumers must perform in deciding whether to assume the risks inherent in taking part in an activity on the Internet involving behavioral targeting. Under Judge Hand's formula, a consumer should be willing to participate in an activity involving behavioral targeting as long as the value the consumer gets from participation exceeds the risk of loss. The risk of loss, just as in the classic tort law analysis, is equal to the probability of loss multiplied by the expected magnitude of the loss.

Consumers are not able to readily determine the risk of loss inherent in participating in activities involving behavioral targeting because they lack accurate information about the probability of the loss and the magnitude of the harm that could occur. Thus, consumers are in a poor position to decide when and how to protect themselves from the harms inherent in behavioral targeting. Indeed, as the foregoing examples have shown, consumers cannot assess the potential magnitude of harm because they likely do not know when profilers are collecting and using their data. Consumers also lack information about what data the profilers collect or guess about them. In addition, consumers are unable to assess the probability of harm occurring because they do not know how profilers use their behavioral profile or the prevalence of inappropriate use or

130. Conway v. O'Brien, 111 F.2d 611, 612 (2d Cir. 1940).

131. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

132. *See id.; See also* JOHN L. DIAMOND, ET. AL., UNDERSTANDING TORTS 69 (2d ed. 2000).

disclosure.[133]

The consumer's inability to accurately assess the magnitude of loss begins with her inadequate understanding of how much data the profilers can obtain and how the data describes even some of the most intimate details about the consumer.[134] Consumer and privacy advocates analogize the non-consensual use of an Internet user's information to a wiretap of a telephone call.[135] They suggest that consumers would rightly be upset if someone listened to their phone conversations without consent, regardless of the purpose of the eavesdropping or the steps used to safeguard the record of the information learned from the eavesdropping.[136] Consumers do not expect their phone calls to be intercepted nor for revealed personal details to be cataloged.[137]

Likewise, consumers do not expect their ISPs to listen in on their web-based "conversations." On the contrary, consumers expect their ISPs to serve merely as a conduit for their information.[138] Similarly, when a consumer visits a website, he expects to receive information and may not expect to be tracked and profiled. Consumer advocates fear that as Internet users begin to understand the extent of the profiling that online marketers perform, they will begin to avoid using the Internet in spite of its efficiency and convenience.[139]

These breaches of consumer expectation may be especially worrisome when profilers collect sensitive elements of personal information that have a heightened potential for abuse. For instance, the FTC notes that financial and health information are especially sensitive.[140] Financial details are rife with the potential for financial fraud.[141] Health information could easily become an embarrassment,

133. *Privacy Impact*, *supra* note 110. *See also* Letter from Alan Davidson, Senior Policy Counsel and Head of U.S. Public Policy, Google Inc. to Jessica Rich, Federal Trade Commission (Apr. 4, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080404google.pdf [hereinafter Google Letter] (explaining that Google is concerned with building trust with users through "transparency" in behavioral advertising, and, in particular, "being upfront with our users about what information we collect and how we use it").

134. *Privacy Impact, supra* note 110.

135. *See Statement*, *supra* note 62, at 16, 21-29.

136. *See id.* at 15-16.

137. *See id.*

138. *See id.* at 1.

139. *Id.* at 8.

140. PRINCIPLES, *supra* note 7, at 42; *see also* Chloe Albanesius, *Should Online Ads Be Allowed to Know If You Have AIDS?*, PC MAGAZINE, Apr. 11, 2008, http://www.pcmag.com/article2/0,2817,2283076,00.asp.

141. *See* PRINCIPLES, *supra* note 7, at 42-44.

an unwelcome intrusion on a consumer's privacy, and might, in an extreme case, even hamper the consumer's ability to get employment or insurance.[142] Privacy advocates are also understandably concerned about the profiling of children, because they may not understand the privacy concerns as an adult might, nor are they capable of legally assenting to a service provider's privacy policy or terms of use.[143] A consumer's physical location is also sensitive because of its significance in allowing the consumer to be personally identified.[144]

Consumers are also likely to be surprised that profilers use mathematical models to "guess" the characteristics of a consumer.[145] Statistical techniques make it possible that a consumer's profile might not only include factual information about a consumer's Internet use, but also inferred information, which may or may not be correct.[146] Because profilers potentially have access to information about the habits, likes, and propensities of many consumers, they may "guess" or "predict" unknown information about consumers through a statistical process of comparing them to other consumers with known information.[147] In a sense, this process is exactly what Amazon or Netflix does when generating suggestions for books, movies, or other items: they suggest to consumers other items that similar consumers (meaning, in this sense, consumers with similar preferences or purchases) liked. But, now, instead of guessing a consumer's preference for a good or service, the profiler guesses information about the consumer.[148]

---

142. *See Privacy Impact, supra* note 110.

143. *See id.*; JEFFREY FERRIELL & MICHAEL NAVIN, UNDERSTANDING CONTRACTS, 509-10 (2004) (noting that, in contract law, children are not capable of "adequately protecting their own interests."). Congress was also concerned, and it expressed that concern when it passed the Children's Online Privacy Protection Act ("COPPA"). *See* 15 U.S.C. §§ 6501-06 (2000). COPPA defines a child as a person under 13, leaving children over the age of 13 without enhanced privacy protection. 15 U.S.C. § 6501 (2000).

144. *Privacy Impact, supra* note 110. The CDT's statement also indicates that the laws that protect health information within the health care sector might not apply outside this context. *Id.*

145. *See* CENTER FOR DIGITAL DEMOCRACY ET AL., ONLINE BEHAVIORAL TRACKING AND TARGETING, LEGISLATIVE PRIMER 3 (2009), http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf [hereinafter PRIMER]; REPORT TO CONGRESS, *supra* note 31, at 5-6.

146. *See* JIAN HU ET AL., DEMOGRAPHIC PREDICTION BASED ON USER'S BROWSING BEHAVIOR 151 (2007), http://www2007.org/papers/paper686.pdf (last visited Feb. 10, 2011) (proposing a method for predicting basic demographic information of consumers on the internet).

147. *See id.* While it is not known how prevalent these inferential techniques are today, the existence of the research attests to the value of making guesses about key demographic characteristics of consumers that enable improved ad targeting.

148. HU, *supra* note 146, at 1; REPORT TO CONGRESS, *supra* note 31, at 4-6.

Because consumers lack marketers' sophisticated understanding of the models that can be used to predict a consumer's demographic information, their intuitive assessment of the magnitude of the harm of participating in an Internet activity involving behavioral targeting is likely to be too low. If inferred demographic characteristics are stored along with other elements in a consumer's profile as factual information, and then inappropriately disclosed, even inadvertently, it could make the magnitude of embarrassment even worse. Even when the inferred information is accurate, it allows profilers to create an even more comprehensive profile of a consumer that contains information the consumer did not even know he or she was disclosing.[149]

For instance, researchers at the Massachusetts Institute of Technology, after analyzing over 4,000 students' Facebook profiles, were recently "able to predict, with 78 percent accuracy, whether a profile belonged to a gay male."[150] The inference about a person's sexuality, if it is unexpectedly or inappropriately disclosed, could be deeply intrusive, embarrassing, and harmful for consumers, regardless of whether the inference is correct.

Thus, because consumers lack information about what information profilers collect (or guess) and how sensitive the information is, consumers are likely to underestimate the magnitude of harm that can occur because of their participation in activities that involve behavioral targeting. However, consumers have even less information to aid them in understanding the likelihood that harm will occur.

For instance, in May 2010, Facebook "users discovered a glitch that gave them access to supposedly private information in the accounts of their Facebook friends, like chat conversations."[151] This presents consumers with the difficult question of trying to assess the likelihood that a company like Facebook will disclose their personal data in a way that can harm them. As an industry analyst noted, "[Facebook users] have to ask whether it is a platform worthy of their trust."[152] And a recent complaint against Facebook in the FTC even charged that Facebook also intentionally "manipulate[s] the privacy settings of users and its own privacy policy so that it can take

149. *See* PRIMER, *supra* note 145, at 3.

150. Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 17, 2010, at A1.

151. Jenna Wortham, *Facebook Glitch Brings New Privacy Worries*, N.Y. TIMES, May 6, 2010, at B1.

152. *Id.*

personal information provided by users for a limited purpose and make it widely available for commercial purposes."[153] Facebook users are especially indignant about the inadvertent disclosure because "most people signed up for Facebook with the understanding that their information would be available only to an approved circle of friends."[154]

The Facebook example is simply an unusually public example of an inadvertent data breach. As part I.B.2 described, there is ample anecdotal evidence showing that data breaches happen continually under a variety of circumstances. The typical consumer simply has no way of intelligently assessing the thoroughness of the precautions that a profiler takes to protect the consumer's data. Consequently, the consumer simply cannot assess the probability that a profiler's use of behavioral targeting will harm them.

4. Mitigation Through Anonymization

Profilers have attempted to mitigate some risks of harm to consumers through anonymization.[155] Anonymization is an effort to take a set of data, such as a database containing consumer profiles, and eliminate those characteristics of the set that would allow someone to discern the identities of the consumers described in the dataset.[156] Behavioral advertisers, during public hearings and proceedings before the FTC, expressed their belief that information that does not identify a consumer's identity poses no significant risk to the consumer's privacy.[157] Other behavioral advertisers have touted their efforts to anonymize their data by severing the direct ties between a consumer's profile and the consumer's identity.[158] Indeed, behavioral advertisers often have little need to know the identity of a consumer to effectively profile and advertise to that consumer.[159] Of

153. *Id.*

154. *Id.*

155. *See, e.g.*, Google Letter, *supra* note 133, at 8; Complaint at 24, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/.

156. Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, at 111-12, PROCEEDINGS OF THE 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2008), *available at* http://userweb.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf, at 1-2.

157. PRINCIPLES, *supra* note 7, at 20-21.

158. Google Letter, *supra* note 133, at 8 (noting Google's decision to anonymize IP addresses and cookie-based identification numbers after 18 months, even when these are not personally identifying, because "we believe that our users would prefer that we further anonymize this data after a reasonable period of time.").

159. *DoubleClick*, 154 F. Supp. 2d at 503-05 (describing how DoubleClick engages in

course, anonymization would mean, at a minimum, the elimination of obviously identifying information, like a consumer's name, address, social security number, e-mail address, phone number, and so forth.[160]

But computer scientists caution that even in datasets where this obviously identifying information has been removed, it is remarkably easy to identify particular users.[161] Researchers were able to identify the users associated with anonymized information from the Netflix Prize dataset using data gleaned from IMDB (a movie-related website that offers users the opportunity to rate movies).[162] Netflix offered the Prize to any researcher who could improve Netflix's movie suggestion technique by a designated margin, and could demonstrate that improvement on a sample "anonymous" dataset of consumers' movie ratings that Netflix made available.[163] The researchers found that if they disregarded an anonymous consumer's favorable ratings of the 100 most popular movies from the Netflix data, the pattern of consumer likes and dislikes was fairly unique.[164] Then, through correlation of this pattern of unique likes and dislikes (between the Netflix and IMDB data), the researchers were able to discern the consumers' identities.[165] And, although Netflix's anonymization efforts may have been incomplete, the scientists suggest that their methods for reconstructing consumers' identities from anonymized data would have worked even if Netflix had modified dates, added deliberate errors, or taken other steps to obfuscate the consumers' identities whose preferences the data described.[166] Netflix cancelled plans for a second Netflix Prize because of the attendant privacy concerns.[167]

Other researchers have come to similar conclusions. Stanford University researchers have reported that a date of birth is highly

---

behavioral advertising without knowing a user's identity).

160. *See id.*

161. *Id.*

162. *Id.*

163. Netflix, Netflix Prize, http://www.netflixprize.com (last visited May 12, 2009).

164. Bruce Schneier, *Why 'Anonymous' Data Sometimes Isn't*, WIRED.COM, Dec. 13, 2007, http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213 (describing the Narayanan and Shmatikov work).

165. *Id.*

166. *Id.* When a reputable organization like Netflix fails to implement effective anonymization of a dataset that they intended to publicly release, it is easy to imagine other profilers making the same mistake in the maintenance of their own profiles, especially if they do not anticipate researchers and others testing the anonymization.

167. Lohr, *supra* note 150.

valuable when attempting to discern someone's identity.[168] Other researchers have concluded that about half of the U.S. population can be identified using only their gender, date of birth, and the city of residence.[169] In essence, even information that does not appear to disclose a person's identity can readily do so when combined with other data.[170]

Indeed, the AOL dataset that led to the *New York Times* reporters' identification of Ms. Arnold was anonymized before AOL released it for scholarly study.[171] AOL later apologized and removed the data, which they claimed had not been duly authorized for release.[172] Because of the release, AOL's chief technology officer resigned and AOL fired a whole team of researchers.[173]

C. The Benefits of Behavioral Targeting

While the privacy concerns associated with behavioral targeting are significant, the benefits of this technology are compelling and far less contingent than the risks. Behavioral advertising, for instance, is one way of funding the generation and delivery of content on the Internet.[174] Other forms of behavioral targeting promise to connect consumers with old friends, new friends, and useful products the consumer will likely enjoy. Internet businesses are already using behavioral targeting to provide these benefits to consumers. On the other hand, the risks associated with behavioral targeting are largely contingent on some kind of unexpected or improper behavior, such as an inappropriate disclosure or misuse of consumer profile data. Thus, if the risks of harm to consumers can be effectively managed, and service providers share the benefits of the technology with their customers, the technology benefits both profilers and consumers.

Behavioral advertising, for instance, allows content providers to fund the delivery of web-based content and services to consumers on the Internet.[175] One way of providing web-based content is to require

168. Schneier, *supra* note 164.

169. *Id.*

170. *Id.*

171. *Id.*

172. *Id.*

173. Schneier, *supra* note 164.

174. *See infra* notes 176-78.

175. Google Letter, *supra* note 133, at 2; *Behavioral Advertising: Industry Practice and Consumers' Expectations Before the Joint Hearing of the Subcomm. on Communications, Technology and the Internet and the Subcomm. on Commerce, Trade and Consumer Protection of the H Comm. On Energy and Commerce Committee* , 111th Cong. 3 (2009), *available at*

consumers to pay directly for the service (a "subscription-based" approach).[176] Another is to follow the broadcast television model of allowing advertising to pay content providers for providing a service to consumers (an "advertising-based" model).[177]

The advertising-based approach is advantageous for both advertisers and consumers. Behavioral advertising, as compared to other forms of advertising, offers advertisers an efficient method of precisely targeting a valuable demographic.[178] It is, in fact, so efficient that it offers companies "the highest return on investment for dollars spent on e-advertising–a value that is only diminished by the controversial nature of [the] tracking technology."[179] Consumers respond to this new technology. They are "at least ten percent more receptive to behaviorally targeted advertisements than to contextually targeted advertisements."[180] The market for behavioral advertising is expected to grow "from $350 million in 2006 to $3.8 billion by 2011."[181] The technology also helps small businesses compete, even when their customers would ordinarily be too diffuse to reach through other advertising outlets.[182]

Indeed, Microsoft's CEO, Steve Ballmer lauded the technology: "The more we know about customer behavior, the more every ad is relevant."[183] This relevance works both ways. Of course, this relevance means that the advertiser is able to use its advertising budget to target those customers it most wishes to reach. But it also means that when a consumer sees an ad, it is more likely to be

---

http://energycommerce.house.gov/Press_111/20090618/testimony_toth.pdf (Testimony of Anne Toth, Vice President of Policy and Head of Privacy, Yahoo! Inc.); PRINCIPLES, *supra* note 7, at 1 ("[Consumers] may also benefit, however, from the free content that online advertising generally supports, as well as the personalization of advertising that many consumers appear to value.").

176. Hotaling, *supra* note 13, at 540.

177. *Id.*

178. *Id.* at 533-38.

179. *Id.* at 536.

180. *Id.* at 538 (quoting Tameka Kee, *Revenue Science Finds Behavioral Targeting Ads 22% More Effective*, MEDIAPOST PUBLICATIONS, Sep. 12, 2007, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=67293). Contextually targeted advertisements are those that are targeted without the use of a consumer profile; PRINCIPLES, *supra* note 7, at 29 ("[C]ontextual advertising differs from behaviorally targeted advertising because it is based only on the content of a particular website or search query, rather than on information about the consumer collected over time.").

181. Hotaling, *supra* note 13, at 539.

182. Google Letter, *supra* note 133, at 2. This efficiency is especially true when one thinks of the limited advertising budgets of small businesses–especially new small businesses.

183. Hotaling, *supra* note 13, at 536-37.

relevant (and therefore *useful*[184]) to him or her.[185] Consumers will see ads that are more likely to be appealing, useful, and appropriately tailored to their sensibilities.[186] Revenue resulting from the ad's placement then can fund Internet-based content and services.[187] Google credits revenue from online advertising for funding its free e-mail, search, and geographic information services.[188]

Consumers already reap the benefits of free services funded through behavioral advertising.[189] In spite of the potential for profiling to harm consumers, the prevalence of harm stemming from profiling appears quite low.[190] This is not to say that abuse and misuse do not occur. But, considering the concrete and widespread benefits that behavioral targeting already provides, it makes little sense to enact a remedial scheme that hampers the advancement of a generally helpful technology.[191] Indeed, behavioral advertising is already being used to aggregate a commodity–consumer information–that, to the individual consumer, has little exchange value into a valuable product that allows the consumer to access relevant and free Internet content.[192]

And, the benefits of behavioral targeting are not limited to the behavioral advertising context. Other forms of behavioral targeting also provide benefits for consumers. Facebook uses consumers' profiles to connect its customers to other potential acquaintances. Amazon suggests products that consumers might enjoy.[193] Netflix suggests movies the consumer might enjoy. Not only are these

184. Google Letter, *supra* note 133, at 2.

185. *See* PRINCIPLES, *supra* note 7, at 1, 6, 9-10.

186. *Id.*

187. *Id.*; Google Letter, *supra* note 133, at 2.

188. Google Letter, *supra* note 133, at 2.

189. *Id.*

190. *See* Bennet Kelley, *Privacy and Online Behavioral Advertising*, 11 J. OF INTERNET LAW 24, Dec. 2007 (noting that a "recurring theme" during the FTC's hearings was "the failure of those advocating further regulation to demonstrate any specific instances of harm."). One of the FTC's Commissioners, Mozelle Thompson, is reported as saying "the FTC should not take any action at all in the absence of evidence of consumer harm." *Id. See also* Diane Bartz, *FTC Urged to Limit Behavioral Advertising*, EWEEK, Apr. 18, 2008 (reporting that the American Advertising Federation, Association of National Advertisers, and other organizations had issued a statement asserting that "any additional principles or guidelines should be issued only after the [FTC] specifically identifies harms and concerns so that business is in a position to consider and address them").

191. *See* Kelley, *supra* note 190; Bartz, *supra* note 190.

192. Consumer data may have little exchange value, but obviously has other value for consumers.

193. Amazon.com, Help, http://www.amazon.com/gp/help/customer/display.html (last visited May 12, 2009).

benefits compelling, but they come without some of the dangers associated with behavioral advertising. For instance, consumers often volunteer the information the companies use to make these recommendations.[194] Often, a consumer can see why a website offered a particular recommendation.[195] Of course, even this form of profiling is not without privacy risks. In fact, the risks may be greater; companies like Amazon and Facebook store personally identifying information about consumers (name, address, phone number, and e-mail), so the risks of identity theft and embarrassment are heightened with respect to the unexpected disclosure of this data.

The benefits of behavioral targeting are, in fact, so compelling that some Internet service providers have attempted to appropriate for themselves the financial benefits of behavioral advertising. A recently filed complaint in California alleges that several Internet service providers (ISPs) are using the deep packet inspection form of behavioral advertising to turn their clients' data into a revenue stream for themselves, even though the ISP's clients are already directly paying for service.[196] These ISPs are using a device from NebuAd[197] that plugs directly into the ISP's network equipment, allowing the equipment access to all Internet data sent to and from any and all of the ISP's customers.[198] The complaint also alleges that adequate notice was not given to the customers whose Internet traffic was rigorously deconstructed, examined, analyzed, and manipulated.[199] The complaint further alleges that following an opt-out procedure did not actually opt the consumer out of this process of constant inspection of his or her Internet traffic.[200] Similar allegations are levied, in the United Kingdom, against British Telecom and Phorm, another seller of deep packet inspection appliances.[201] British

194. *E.g.*, *id.*

195. *E.g.*, *id.*

196. Complaint at 23, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ (according to Bob Dykes, NebuAd's CEO: "The ISPs have not been able share in ad revenue and wealth creation around the publishing side of the internet.").

197. *Id.* at 16-17.

198. *Id.*; *See generally supra* Part I.A.

199. Complaint at 36, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/.

200. *Id.* at 24-25. The opt-out procedure allegedly prevented the consumer from receiving targeted ads, but did nothing to stop the NebuAd appliances from performing deep packet inspection on all of the data the consumer sent to or received from devices on the internet. *Id.*

201. Kevin J. O'Brien, *Use of Web Tracking Tool Raises Privacy Issue in Britain*, N.Y.

Telecom admits that it did not obtain consumers' consent to employ these appliances.[202]

II. LAWS APPLICABLE TO BEHAVIORAL TARGETING

The legal rules that presently apply to behavioral targeting cannot effectively deter improper use of consumer information or compensate victims when abuse or misuse occurs. To be sure, there are a variety of laws that may apply to provide redress for those who suffer significant harm from behavioral targeting, but plaintiffs seeking redress have failed, so far, to convince the courts that behavioral targeting violates their rights.[203] And, often, a viable private lawsuit will be insurmountably difficult for a typical plaintiff to bring.[204] Public enforcement, in the form of the FTC enforcement action, is also rare and appears to be confined to the most egregious cases.[205]

Because profilers' collection practices often operate in a manner invisible to the consumer, it is difficult for consumers to bring private suits; even when a consumer suspects that she has been harmed, the consumer may not know who to sue, and may lack the evidence necessary to prove liability and damages.[206] The consumer who sees an ad may not know whether it is a behavioral ad, nor does the consumer even necessarily become aware of which advertisers are profiling.[207] The consumer also does not know the content of her profile.[208] Moreover, because behavioral advertisers need not and often do not know a consumer's identity,[209] a plaintiff faces a difficult, if not completely insurmountable, challenge to match inappropriately disclosed data to a suspected source to prove

---

TIMES, Apr. 14, 2009.

202. *Id.*

203. *In re* DoubleClick, 154 F. Supp. 2d at 526-27.

204. Hotaling, *supra* note 13, at 559.

205. *See infra* Part III.D.

206. *See In re* DoubleClick, 154 F. Supp. 2d at 526 (dismissing the plaintiffs' claims in part because their Computer Fraud and Abuse Act claim did not support a sufficient claim for damages).

207. *See* PRINCIPLES, *supra* note 7, at 33-37.

208. *Id.* Not only do consumers not know the contents of profiles in a general sense (i.e. what sort of information a profiler collects), but they are unable to know the contents in a specific sense (i.e. "What specific information does the profiler have in their database about me?"). *But see* Stephanie Clifford, *Many See Privacy on Web as Big Issue, Survey Says*, N.Y. TIMES, Mar. 16, 2009, at B5 (reporting that Google has plans to allow a consumer to see what data it has collected about the consumer).

209. *In re* DoubleClick, 154 F. Supp. 2d at 503-05 (describing how DoubleClick engages in behavioral advertising without knowing a user's identity).

causation — she cannot merely ask a profiler to produce all information associated with her name.[210] Consumer and privacy advocates argue that behavioral advertisers have cultivated this information gap to avoid legal accountability.[211]

A. Tort Claims

Nonetheless, there are legal theories under which a consumer can seek redress when behavioral advertisers inappropriately collect or disclose consumer data. For instance, most states have adopted the torts of intrusion on seclusion and public disclosure of private facts.[212] Moreover, the torts of defamation, negligence, and trespass to property may also provide some redress to consumers harmed by behavioral targeting.

The restatement of torts describes the first of these legal theories–intrusion on seclusion–as an intentional intrusion "physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns" and subjects the intruder to liability "if the intrusion would be *highly offensive* to a reasonable person."[213] Because the tort targets the intrusion rather than the release of information, it is more likely to be useful to address a profiler's collection of especially private information rather than the information's inappropriate disclosure.[214] The restatement uses a wiretap to illustrate the tort: "A, a private detective seeking evidence for use in a lawsuit, rents a room in a house adjoining B's residence, and . . . taps B's telephone wires and installs a recording device to make a record of B's conversations. A has invaded B's privacy."[215] Behavioral advertising can be likened to wiretapping.[216] Even so, the requirement that the intrusion be "highly offensive to a reasonable person" establishes a high threshold for liability. It is not clear, for instance, that when AOL recorded that Ms. Arnold searched for men near her age, the intrusion would be highly offensive to a reasonable person, particularly if one purpose of the "intrusion" was to allow AOL to satisfy Ms. Arnold's search request.

---

210. *See* Hotaling, *supra* note 13, at 548-49, 558 (observing that opt-in requirements address this problem and that the consumer's lack of knowledge about the profiler and its activities is the most significant barrier to asserting some level of consumer control).

211. *Id.*

212. JOHN L. DIAMOND ET AL., UNDERSTANDING TORTS 451-52 (2d ed. 2000).

213. RESTATEMENT (SECOND) OF TORTS § 652B (1977) (emphasis added).

214. *See id.*

215. *Id.* (based upon Rhodes v. Graham, 37 S.W.2d 46 (Ky. 1931)).

216. *In re* DoubleClick, 154 F. Supp. 2d at 514.

Similarly, the tort of public disclosure of private facts is defined as giving "publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be *highly offensive* to a reasonable person, and (b) is not of legitimate concern to the public."[217] This tort, unlike the tort of intrusion on seclusion, focuses on *publicizing* private data, and would therefore be useful for deterring and redressing inappropriate *disclosure*.[218] However, as with the tort of intrusion on seclusion, the "highly offensive to a reasonable person" standard is a formidable threshold for a plaintiff to overcome.[219] Moreover, the tort requires disclosure to a large group; disclosure to a single person or small group does not trigger liability.[220]

The law of defamation may aid victims of disclosures of false information.[221] Under the law of defamation, a defendant is liable for a published defamatory statement concerning a plaintiff,[222] unless the defendant can prove the statement is true.[223] In addition, the incorrect information must be negligently or intentionally published to some third person.[224] One advantage of a defamation theory is that damages for the emotional distress of the disclosure are often presumed.[225] Because defamation targets false statements, it might be especially valuable for consumers harmed by the disclosure of incorrect inferred information, as described in part I.B.

---

217. RESTATEMENT (SECOND) OF TORTS § 652D (1977) (emphasis added).

218. *See id.*

219. *See id.*

220. *Id.*

221. The likelihood that a consumer's profile would contain false information is difficult to assess. False information could, perhaps, be the result of incorrect inferences. *See supra* Part I.B. It could also be the result of errors in profiling that result from a profiler's inability to accurately distinguish among computer sharers. PRINCIPLES, *supra* note 7, at 22. Regardless of how errors occur, privacy advocates recognize that there are circumstances in which a consumer's profile will not be correct, and a consumer will want to correct the error. Ciocchetti, *supra* note 123, at 37-38. To the extent that errors remain in a profiler's database, some of these errors may rise to the level of actionable defamation.

222. DIAMOND, *supra* note 212, at 432-33. Under the law of defamation, special constitutional rules apply to speech that arguably defames public figures, but I assume in this analysis that the consumer is not a public figure. *Id.* at 442-50.

223. RESTATEMENT (SECOND) OF TORTS § 581A (1977).

224. *See id.* § 558.

225. DIAMOND, *supra* note 212, at 437. Some courts have been unwilling to recognize the dignitary harm stemming from profiling as a harm that the law should remedy, even when consumers are forced as a result of a data breach to monitor their credit reports for indications of financial fraud and identity theft. Sprague & Ciocchetti, *supra* note 101, at 101-02. Thus, the defamation claim's presumption of damages might, in an appropriate case, be quite valuable to the plaintiff.

A negligence theory may also prove useful for redressing harm resulting from data breaches, as long as courts are willing to concur that a profiler owes consumers a duty to take reasonable steps to safeguard their data.[226] Under a negligence theory, a plaintiff would have to prove the breach of such a duty caused the plaintiff's damages.[227] Negligence, however, would provide no redress to consumers whose data is disclosed in spite of a profiler's reasonable efforts to prevent inappropriate disclosure.[228] In one recent data breach case, TJX, a company that experienced a massive data breach not related to behavioral targeting, settled a lawsuit employing the negligence theory for nearly $41 million to compensate banks for their losses from the data breach.[229]

In another recent case, *In Re DoubleClick, Inc. Privacy Litigation*,[230] a class of plaintiffs sought to hold DoubleClick, a cookie-based behavioral advertiser, liable for the tort of trespass to property.[231] The plaintiffs alleged that the defendant's tracking cookies made use of the plaintiffs' own computers to deprive the plaintiffs of their privacy.[232] Generally, the tort of trespass to property requires the plaintiff to show that a defendant has damaged the property or deprived the plaintiff of its use,[233] although defendants are not liable when plaintiffs consent to the trespass.[234] Unfortunately, the federal court declined to hear the supplemental state law tort claim after it dismissed the plaintiffs' claims based on federal law.[235]

B. Federal Statutory Claims

However, the *DoubleClick* plaintiffs principally premised their complaint on alleged violations of three federal statutes.[236] The plaintiffs argued that the placement of tracking cookies on plaintiffs' computers violated these statutes regardless of whether the defendants

226. DIAMOND, *supra* note 212, at 51.

227. *Id.* at 50-51.

228. *Id.* at 51-52.

229. Sprague & Ciocchetti, *supra* note 101, at 98-99.

230. *In re* DoubleClick, 154 F. Supp. 2d. at 497.

231. *Id.* at 500.

232. *Id.*

233. DIAMOND, *supra* note 212, at 21.

234. *See id.* at 34.

235. *In re* DoubleClick, 154 F. Supp. 2d at 526-27 ("When federal claims are dismissed, retention of state law claims under supplemental jurisdiction is left to the discretion of the trial court. . . . We decline to exercise supplemental jurisdiction over plaintiffs' state law claims.").

236. *Id.* at 500.

improperly disclosed the information it learned as a result.[237] Plaintiffs made their first claim under ECPA, or, more specifically, Title II of the Electronic Communications Privacy Act.[238] ECPA "aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications."[239] It provides for punishment for a defendant that "(1) intentionally accesses *without authorization* a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system."[240] The court concluded, however, that DoubleClick's behavioral advertising fell within an exception to the statute's proscriptions for "conduct authorized . . . by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user."[241] The court reasoned that the websites with which the plaintiffs communicated were users of the communication facility and these websites authorized DoubleClick's actions when they incorporated DoubleClick's enabling programming into their websites.[242] Thus, when a website operator consents to the use of cookie-based consumer profiling, and the profiling conforms to the scope of the consent, an aggrieved Internet consumer cannot succeed in an ECPA claim against the profiler.[243]

However, in *In Re Pharmatrak Privacy Litigation*, the plaintiffs' ECPA claims were slightly more successful.[244] The Pharmatrak plaintiffs convinced the court that the defendant company had accessed the plaintiffs' communications (containing their data) without authorization.[245] The defendant, Pharmatrak, Inc., marketed a cookie-based profiling product to pharmaceutical companies that tracked consumers' website visits across several pharmaceutical industry websites for the purpose of allowing industry-wide analysis and comparison of Internet consumer trends.[246] After Pharmatrak collected personally identifying information about consumers in

237. *Id.* at 499.
238. *Id.* at 507.
239. *Id.*
240. *Id.* (emphasis added).
241. *In re* DoubleClick, 154 F. Supp. 2d at 507.
242. *Id.* at 508-10.
243. *Id.*
244. *In re* Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 13 (1st Cir. 2003).
245. *Id.*
246. *Id.*

contradiction of assurances to its pharmaceutical company customers, the court concluded that the interception of consumer data was not authorized.[247] Nonetheless, Pharmatrak escaped liability on remand because the court concluded the interceptions were not intentional.[248]

The *DoubleClick* plaintiffs' Wiretap Act[249] claim fell victim to the same reasoning that undercut their ECPA claim.[250] The Wiretap Act prohibits the intentional interception of an electronic communication, which DoubleClick conceded that it had done.[251] DoubleClick responded, however, that its conduct fell within an exception to liability for wiretaps to which one party consented.[252] The court agreed.[253] It reasoned that although the plaintiffs themselves had not consented, the operators of the websites that the plaintiffs visited consented when they incorporated DoubleClick's enabling programming into their websites.[254]

Finally, the *DoubleClick* plaintiffs also alleged that DoubleClick had violated the Computer Fraud and Abuse Act (CFAA).[255] The CFAA prohibits the intentional access of a computer without authorization or in excess of the authorization.[256] However, the CFAA also limits private causes of action to situations involving "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."[257] The plaintiffs, the court concluded, had not pleaded any facts to suggest that they could show such extensive damages.[258] The court also reasoned that the invasion of the plaintiffs' privacy, trespass to the plaintiffs' personal property, and misappropriation of the plaintiffs' data, even if proven, were not economic losses that could count toward the $5,000 floor.[259] The

247. *Id.*

248. *In re* Pharmatrak, Inc. Privacy Litigation, 292 F. Supp. 2d 263 (D. Mass. 2003) (granting summary judgment because the collection was not intentional). *See also* Hotaling, *supra* note 13, at 548.

249. 18 U.S.C. § 2510, *et. seq.* (2006).

250. *See In re* DoubleClick, 154 F. Supp. 2d at 514.

251. *Id.* at 514.

252. *Id.*

253. *Id.*

254. *Id.*

255. *Id.* at 519-20.

256. *In re* DoubleClick, 154 F. Supp. 2d at 519.

257. *Id.* at 520 (quoting 18 U.S.C. § 1030(e)(8) (2000) (amended 2001)). *See also id.* at 523 (concluding that all damages and losses are subject to the $5,000 floor).

258. *Id.* at 526.

259. *See id.* at 525, n.33.

court's reasoning suggests that DoubleClick's actions were improper, but not enough for a court to provide a remedy under the CFAA.[260]

A currently pending class-action suit, *Valentine v. NebuAd*, also asserts ECPA and CFAA claims against NebuAd, a deep packet inspection-based behavioral advertiser.[261] These claims may be stronger against a deep packet inspection-based profiler (compared to a cookie-based profiler) because the profiler does not obtain any form of consent from either the consumer or the website the consumer visits.[262]

C. Unjust Enrichment Claims

The plaintiffs in both *DoubleClick* and *NebuAd* also made claims under the common law theory of unjust enrichment.[263] Unjust enrichment allows for recovery in situations where a defendant has been unfairly enriched at the plaintiff's expense.[264] Unjust enrichment is a proven basis for liability when a defendant misuses information belonging to the plaintiff for its own purposes.[265] The *DoubleClick* court refused to consider this state law claim after it dismissed the plaintiffs' federal statutory claims.[266] However, the *NebuAd* plaintiffs also make an unjust enrichment claim, alleging that NebuAd "has received and retains information regarding specific purchase and transactional information that is otherwise private, confidential, and not of public record and/or have received revenue from the provision of such information."[267] Further, the *NebuAd* plaintiffs also allege that NebuAd knows of the benefit and "should not be permitted to retain the information and/or revenue which they acquired . . . . All funds, revenues, and benefits received by Defendants rightfully belong to Plaintiffs."[268] So long as the court is willing to recognize that

260. *See id.* at 519-27.

261. *See* Complaint, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/.

262. *See id.* at 24-25.

263. *Id.* at 1; *In re* DoubleClick, 154 F. Supp. 2d at 500.

264. *See* DAN B. DOBBS, LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION 371 (2d ed. 1993).

265. *Id.* at 375 & n.21 (citing e.g., Janigan v. Taylor, 344 F.2d 781 (1st Cir. 1965), *cert. denied*, 382 U.S. 879 (1965)).

266. *In re* DoubleClick, 154. F. Supp. 2d at 526-27.

267. *See* Complaint, Valentine v. NebuAd, Inc., No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/.

268. *Id.* at 48-49.

intercepted communications are a kind of property or benefit that belongs to a consumer, this claim is promising.

Behavioral advertisers have asserted elsewhere, however, that they believe that "consumers do not own the data that [profilers] collect about them, and that there is no precedent for giving consumers the ability to dictate the terms on which they use a website."[269] This approach effectively analogizes consumer information to unowned wild animals or unowned running water, which, at common law, became the property of the person who reduced them to possession.[270] Therefore, according to this line of reasoning, because a profiler exerts the effort to reduce consumer information to possession, the profiler ought to be regarded as the owner.[271] The *NebuAd* court may have to sort out whether the consumer or the profiler has the better claim to the data and the benefits of using it.

D. The Federal Trade Commission

The Federal Trade Commission currently plays a larger role than private plaintiffs in deterring and redressing the inappropriate collection and disclosure of consumer profile information.[272] In the Federal Trade Commission Act, Congress vested the FTC with broad powers to regulate unfair and deceptive trade practices: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[273] However, the Act limits unfairness to situations where "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[274] The FTC reports that it has brought twenty-three actions between 2001 and February 2009 against companies that "allegedly have failed to provide reasonable protections for sensitive consumer information in both online and

269. PRINCIPLES, *supra* note 7, at 31.

270. *See, e.g.*, Pierson v. Post, 3 Cai. R. 175, 177, 178 (N.Y. Sup. Ct. 1805) (concluding that a hunter who spirited away an injured fox was the first to reduce it to possession).

271. *See, e.g., id.* at 178 (concluding that wild animals become property when reduced to possession); Int'l News Serv. v. Associated Press, 248 U.S. 215, 236 (1918) (concluding that, while nobody can own the news, the efforts to gather fresh news confer on the gatherer a quasi-property right relative to competitors only).

272. See PRINCIPLES, *supra* note 7, at 5 n.8.

273. 15 U.S.C. § 45(a) (2006) (known as § 5 of the Federal Trade Commission Act).

274. *Id.* at § 45(n)

offline settings."[275] While this may sound impressive, it amounts to only about eight actions per year.[276] The FTC has, however, indicated that it intends to continue to use its authority to secure compliance when companies fail to implement reasonable measures to address the privacy and security risks to consumers' information.[277] Similarly, the FTC has signaled it will also investigate companies that use collected data in a manner inconsistent with the privacy policies or other agreements under which the data is collected.[278] Finally, the FTC also "intends, where appropriate, to initiate investigations of possible unfair or deceptive acts or practices in this area that would potentially violate . . . the FTC Act."[279]

The FTC also enforces the provisions of the Child Online Privacy Protection Act, or COPPA.[280] COPPA is intended to prevent websites from obtaining personal information from children without parental consent.[281] It also puts parents in a position of control over their children's personal information.[282] COPPA requires website operators to provide, on parental request:

> (i) a description of the specific types of personal information collected from the child by that operator; (ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and (iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child.[283]

Because COPPA gives parents the right to refuse an operator permission to continue to collect or use already collected information, and to see what information the operator has collected, COPPA gives parents far more control over their children's privacy than adults have, even under the FTC's recently-issued self-regulatory

---

275. PRINCIPLES, *supra* note 7, at 5 n.8.

276. *See also* Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled With Fair Information Practices,* 26 J. MARSHALL J. COMPUTER & INFO L. 1, 27 (2008) ("[T]he FTC has brought fewer than thirty actions over the past ten years.").

277. *See* PRINCIPLES, *supra* note 7, at 19.

278. *See id.*

279. *Id.* at 20.

280. 15 U.S.C. § 6501, et. seq.

281. *See id.* at § 6502.

282. See *id.* at § 6502(b) (requiring the FTC to enact regulations that "collect[] personal information from children" to "obtain verifiable parental consent for the collection, use, or disclosure" of that information).

283. *Id.* at § 6502.

principles.[284]

The FTC has enforced this law and its own rules made under COPPA's mandate for agency rulemaking.[285]

III. THE FTC'S SELF-REGULATORY PRINCIPLES

Because the FTC is charged with the regulation of unfair or deceptive acts or practices, the FTC recently issued a set of self-regulatory principles to guide companies that engage in behavioral advertising.[286] The principles were also intended to assuage privacy concerns stemming from the FTC's approval of the Google/DoubleClick merger.[287] The process began with a two day "Town Hall" event intended to facilitate a public discussion about the benefits and privacy risks associated with behavioral advertising.[288] Then, the FTC drafted a set of proposed self-regulatory principles and published them for comment.[289] After receiving a wide variety of comments, the FTC issued a final set of self-regulatory principles.[290] The FTC process is laudable because the self-regulatory principles advance consumers' privacy interests in a way likely to be reasonably acceptable to behavioral advertisers. The principles are clear and relatively detailed.[291] Therefore, they are likely to reduce the privacy risks associated with behavioral advertising across all companies that endorse and follow them.[292]

This part first discusses the scope of the principles, and then proceeds to a discussion of each of the four principles: (1) "meaningful disclosure," (2) "reasonable data security measures," (3) "affirmative express consent" to "material changes to privacy policies," and (4) "affirmative express consent before [using] sensitive data."[293]

---

284. *Compare id.* § 6502 *with* PRINCIPLES, *supra* note 7, at 46-47.

285. *See, e.g.*, United States v. Industrious Kid, No. CV 08-0639 (N.D. Cal. Jan. 28. 2008), *available at* http://www.ftc.gov/os/caselist/0723082/080730comp.pdf.

286. PRINCIPLES, *supra* note 7, at iii.

287. Bartz, *supra* note 190.

288. PRINCIPLES, *supra* note 7, at i-ii.

289. *Id.* at ii.

290. *Id.*

291. *See id.* at 30-48 (describing the need for each of the principles, and what advertisers must do to comply with the principles).

292. *See id.* at 11 (conceding that existing self-regulatory efforts "had not provided comprehensive and accessible protections to consumers" and that the FTC intended the principles to "guide industry in developing more meaningful and effective self-regulat[ion]."

293. *Id.* at 11-12.

A. Scope of the Principles

Unfortunately, the self-regulatory principles do not fully address the harm associated with behavioral targeting. They exclude from their scope several forms of behavioral targeting, even though these forms of targeting pose the same risks as all forms of consumer profiling.

First, the FTC has eliminated all non-advertising behavioral targeting from the principles' applicability.[294] The FTC has sought information on "the potential uses of tracking data other than for behavioral advertising,"[295] but not yet received a robust level of information on these uses.[296] Therefore, the principles do not address any of the privacy risks associated with consumer profiling for purposes other than behavioral advertising.

However, the principles do apply to any behavioral advertiser that "track[s] consumers' online activities to deliver advertising that is targeted to individual consumers' interests."[297] This statement appears to apply to the "spyware" and deep packet inspection-based advertisers, such as NebuAd and Phorm, even though the FTC's principles primarily focus on the cookie-based network advertisers, such as Google/DoubleClick.

Nor do the principles apply to contextual advertising, which is nothing more than the display of an advertisement targeted to a consumer based on the content of a webpage the consumer visited.[298] Because contextual advertising does not involve the compilation and storage of a profile of consumers' behavior, the FTC concluded it did not pose the same risk of privacy-related harms as behavioral advertising.[299]

The principles also do not apply to "first party" targeting.[300] The FTC observed that consumers value a variety of practices that require websites to collect data directly from the consumer, such as "product recommendations, tailored content, shopping cart services, website design and optimization, fraud detection, and security."[301] The FTC

294. PRINCIPLES, *supra* note 7, at 20 ("[T]he Principles apply broadly to companies engaged in online behavioral advertising.").

295. *Id.* at 12.

296. *Id.* at iv.

297. *Id.* at 20.

298. *Id.* at 29.

299. *Id.*

300. *Id.* at 26. *See generally supra* Part I.A.

301. PRINCIPLES, *supra* note 7, at 20.

concluded that these activities are more likely to be consistent with consumer expectations.[302] For instance, on a site like Amazon.com that offers recommendations based on past purchases, the consumer supplies the information that the website uses to make suggestions directly to the website.[303] Therefore, the consumer is better able to understand what data was used to generate the advertisement.[304] Further, consumers can raise any objections with these websites, since consumers know their identities.[305] The FTC also reasoned that while the principles may not apply, the FTC Act still allowed the FTC to regulate these companies' information security practices and privacy policy compliance.[306]

Finally, the FTC decided that the principles *would* apply to the collection of both personally identifying information ("PII") and information that is not personally identifying ("NPII").[307] While industry groups argued that NPII poses little risk of privacy-related harm to consumers, the FTC concluded that it could draw no distinction between PII and NPII because the two can sometimes be merged, and because, as previously discussed, it is increasingly possible to identify consumers based only on data that is considered NPII.[308] The FTC also concluded that there was a distinct privacy risk associated with NPII: behavioral advertising methods at present cannot reliably distinguish among computer sharers, so there is a risk that stored NPII for one person might result in ads that essentially compromise that person's privacy to other users of the same computer.[309] Lastly, the FTC concluded that consumers' privacy concerns were not limited to PII, and that consumers would not want protection limited to PII.[310]

Nevertheless, the FTC chose to limit the principles' scope to information "that reasonably could be associated with a particular consumer or with a particular computer or device."[311] The FTC largely left behavioral advertisers to evaluate for themselves the factual circumstances of their data collection practices and to draw

302. *Id.*
303. *Id.* at 27.
304. *Id.*
305. *Id.*
306. *Id.* at 28 n. 57.
307. *Id.* at 20-21.
308. *Id.* at 22-23.
309. *Id.* at 23.
310. *Id.* at 23-34.
311. *Id.* at 25.

their own conclusions about which data the principles apply to.[312] Consumers are therefore left to bear the risks of profilers' mistaken or self-serving conclusions.[313]

B. Transparency and Consumer Control

The first of the FTC's principles addresses the "transparency" problem.[314] It requires websites that collect behavioral advertising data to (1) state that they are doing so and (2) allow consumers to opt out of this collection.[315] It also requires behavioral advertisers who collect data outside the "traditional website context" to "develop alternative methods of disclosure and consumer choice that meet the standards described above."[316] The disclosure should be "clear, concise, consumer-friendly, and prominent."[317]

The FTC did not prohibit behavioral advertisers from placing the required disclosures in a website's privacy policy, even though "privacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers."[318] The principles encourage alternative methods of disclosure, such as locating the disclosure in proximity to behavioral ads.[319]

The FTC also did not prohibit websites from conditioning use of a website on the consumer's permission to conduct behavioral advertising.[320] This raises the serious concern that consumer control under this principle will be illusory. Indeed, since advertising generates the revenue that makes many websites' content possible, these websites need to have consumers who help them pay for their operations.[321] Websites may therefore refuse to serve customers who opt out. If consumers have nothing more than a "take-it-or-leave-it" choice, they have little real choice.

---

312. PRINCIPLES, *supra* note 7, at 25.

313. *See id.*

314. *Id.* at 30. This problem is really a need for opacity, not transparency, because behavioral advertising is in fact already so "transparent" that a consumer cannot see that it is happening! *See id.* at 31-32 n.62.

315. *Id.* at 46. Of course, the stronger protections inherent in an opt-in system would be consistent with this principle as well. *Id.* at 32, n. 63.

316. *Id.*

317. *Id.*

318. PRINCIPLES, *supra* note 7, at 34-35.

319. *Id.*

320. *See id.* at 30-37.

321. *See* Google Letter, *supra* note 133, at 2.

C. Reasonable Security and Limited Retention of Consumer Data

The FTC's second principle calls for reasonable security and limited retention for consumer data.[322] The appropriate level of security is commensurate with the data's sensitivity, the nature of the "company's business operations," the risks a company faces, and the reasonable protections available to the company.[323] Further, companies must retain data only as long as is necessary to fulfill a "legitimate business or law enforcement need."[324] In establishing this principle, the FTC rejected without explanation consumer and privacy advocates' invitations to establish an explicit retention period or a requirement that retained data be anonymized.[325] Likewise, the FTC puzzlingly rejected the notion that data should be retained only for as long as was needed to fulfill the business purposes explained to the consumer when the data was collected.[326]

D. Express Consent for Retroactive Changes to Privacy Promises

The FTC's third principle requires companies to obtain "affirmative express consent" prior to using data "in a manner materially different from promises the company made when it collected the data."[327] This principle protects consumers from unexpected changes in the way profilers handle their information. Some profilers, worried about the burdens of compliance, had chosen to operate without a privacy policy.[328] Others, however, chose to implement "a privacy policy filled with legalese and loopholes, subject to amendment at any time."[329] Of course, when a profiler can change its privacy policy without notice, the privacy policy does little to educate consumers about how the profiler uses the data it collects.[330] The FTC also explicitly notes that this principle protects

---

322. PRINCIPLES, *supra* note 7, at 46.

323. *Id.*

324. *Id.*

325. *Id.* at 37-38.

326. *Id.*

327. *Id.* at 47. The FTC does not explain how "affirmative express consent" is different than "express consent." *See id.* What form of consent isn't affirmative? *But see id.* at 44, n. 77 ("[P]re-checked boxes or disclosures that are buried in a privacy policy or uniform licensing agreement are unlikely to be sufficiently prominent to obtain a consumer's 'affirmative express consent.'").

328. *See* Sprague & Ciocchetti, *supra* note 101, at 126.

329. *Id.*

330. *See* Ciocchetti, *supra* note 123, at 19, 34.

consumers when profilers' privacy policies or data usage policies change as a result of corporate mergers.[331]

E. Express Consent to Use Sensitive Data

The FTC's final principle dictates that "[c]ompanies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising."[332]

The FTC chose, in adopting this principle, to avoid a concrete definition of "sensitive data."[333] The commenters to the draft principles did not agree on any definition of sensitive.[334] Therefore, while noting that "financial data, data about children, health information, precise geographic location, and Social Security numbers are clearest examples" of sensitive data, the FTC invited stakeholders to "develop more specific standards to address this issue."[335] The FTC rejected the idea of a complete ban on the collection of sensitive data for behavioral advertising.[336]

The wording of this principle is unfortunate because it suggests that the consent that consumers must give is "to receive such advertising" rather than to the *collection* of sensitive consumer data for advertising purposes.[337] This wording suggests that the consumer need only understand and consent to the kind of advertising the consumer will receive, rather than requiring the profiler to obtain consent to collect the supporting sensitive data.[338] Based on the FTC's stated concerns in enacting the principle,[339] the latter approach makes more sense. The FTC should clarify this point in the future.

IV. PROPOSALS TO INCREASE PRIVACY AND CONSUMER CONTROL

The vast majority of the proposals that address the potential

331. PRINCIPLES, *supra* note 7, at 47.

332. *Id.*

333. *Id.* at 42.

334. *Id.* at 44.

335. *Id.* at 44.

336. *See id.* at 43.

337. PRINCIPLES, *supra* note 7, at 47.

338. *See id.*

339. *See id.* at 42-44. The FTC, in particular, notes that protection is needed when consumers believe "that they are searching anonymously for information about medications, diseases, sexual orientation, or other highly sensitive topics." *Id.* at 44. Consent directed at the advertisement rather than the collection of the sensitive data would not address this problem. *See id.*

harm stemming from behavioral targeting have focused on improving the notice that consumers receive about the targeting and giving the consumer more explicit choice about whether to participate in the behavioral targeting. Indeed, a few of these proposals strengthen consumer choice to a degree likely to seriously undercut behavioral targeting-based Internet business models. Some of the proposals also require profilers to safeguard the data they collect. None of the existing proposals, however, truly give consumers a reasonable understanding of the magnitude of potential harm or the likelihood that harm will occur under the adaption of the Learned Hand formula proposed in Part I.B.3.

A. Existing Proposals

Scholars, lawyers, and consumer and privacy advocates have suggested a variety of ways to strengthen consumers' privacy protections. Some of these proposals predate the FTC's self-regulatory principles.

1. Opt-in Consent and Do Not Track Lists

These are two of the most mentioned ideas for improving consumers' control over their information. The concept of opt-in consent requires that profilers obtain consent from a consumer prior to collecting data from the consumer.[340] The idea is attractive because it forces profilers to disclose the desired profiling before data collection and requires consumers to approve of it, which likely also identifies the advertiser.[341]

The "do not track" list is an idea analogous to the "do not call" list the FTC maintains to allow consumers to opt out of telephone marketing.[342] It would allow a consumer who wishes to avoid all behavioral advertising (or perhaps even all behavioral targeting) to indicate his preferences in a way that all profilers would be legally compelled to read and obey.[343]

While these ideas sound appealing, and may indeed be worthwhile, there are two main problems with them. The first problem is technical; the second is economic. Most likely, a consumer's preference to opt in or participate in a "do not track" list

340. Hotaling, *supra* note 13, at 557-58.

341. *Id.*

342. Privacy Letter, *supra* note 93, at 4.

343. *Id.*

would be managed using a cookie.[344] Unfortunately, a consumer would have to repeat the enrollment process any time the consumer used a new device, a new web browser, or after a consumer cleared the cookies in her web browser.[345] It might be difficult for consumers to keep track of these cookies, which are designed for transparency to the user. This technical difficulty could lead to increased confusion among consumers. However, technical problems like these may have easy-to-implement technical solutions.[346] For example, a web browser could automate the process of ensuring a "do not track" cookie is present, or a convention could be adopted for profilers to set opt-in cookies that would allow web browsers to distinguish them from other cookies.[347] Then, when the consumer cleared stored cookies from the web browser, or installed a new web browser, the consumer could choose whether to erase or automatically re-create the specially designated cookies.[348]

The economic challenge is far more difficult. As mentioned above, Internet content providers that rely on advertising for revenue have no incentive to serve a customer who has opted out or refused to opt in to the content provider's ad regime.[349] These customers would tax resources with little or no return. A "do not track" list escalates this problem to an extreme scale. Presumably, many consumers would be attracted to the increased privacy offered by the "do not track" list, and would sign up. Consequently, the pool of revenue-generating consumers available to Internet content providers would decrease radically in size. Content providers would be forced to exclude consumers who refused to participate in the provider's behavioral advertisement regime. This exclusion has the potential to sharply curtail the proliferation of innovation and information on the Internet.[350] And it gives consumers a ridiculous choice: use the advertising-based services on the Internet and lose control of your personal information or choose not to use any of these services.

---

344. *See* PRINCIPLES, *supra* note 7, at 34; Hotaling, *supra* note 13, at 554-55.

345. *See* PRINCIPLES, *supra* note 7, at 34; Hotaling, *supra* note 13, at 554-55.

346. PRINCIPLES, *supra* note 7, at 34; Hotaling, *supra* note 13, at 554-55.

347. *See* PRINCIPLES, *supra* note 7, at 34; Hotaling, *supra* note 13, at 554-55.

348. *See* PRINCIPLES, *supra* note 7, at 34; Hotaling, *supra* note 13, at 554-55.

349. *Supra* Part IV.B.

350. *See* Andrew McCormick, *In-depth TV – Personalized ads herald future of TV*, REVOLUTION 8 (Jan. 9, 2009) (predicting that the improved efficiency of behavioral advertising could drive television programming to the Internet).

2. New York Legislation

In March 2008, a draft bill in the New York legislature would have strengthened privacy protections.[351] It flatly prohibited third-party marketers from using "sensitive medical, financial or sexual personally identifiable information or Social Security numbers" in behavioral advertisements.[352] It also required that marketers "obtain online preference marketing data from reliable sources," "protect online preference marketing data," and "impose online privacy guidelines on PII recipients."[353] Significantly, the bill may also have imposed a modest anonymization requirement: "Non-PII that third-party entities use for online preference marketing may not be linked to a particular individual."[354] Of course, with New York's sizable population, the bill, if enacted, would have been likely to protect consumers far outside New York's borders.[355]

3. Failed Federal Legislation

In 2007, U.S. Senator Patrick Leahy sponsored legislation that would have imposed stronger controls on the collection and storage of consumer information.[356] The bill would impose "requirements for a personal data privacy and security program on business entities that maintain sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons."[357] It also "require[d] [covered] business entities to:

> (1) implement a comprehensive personal data privacy and security program to ensure the privacy, security, and confidentiality of sensitive personally identifying information and to protect against breaches of and unauthorized access to such information; (2)

---

351. David Bender, *Do Behavioral Ads Endanger Your Privacy?*, NEW YORK LAW JOURNAL, Apr. 2, 2008, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1207065969592 (last visited 12/17/2010).

352. *Id.*

353. *Id.*

354. *Id.*

355. *Id.* However, that protective effect may have constituted an unconstitutional burden on interstate commerce under the commerce clause of the United States Constitution. Ryan Paul, *NY Bill Would Police Intersection of Online Ads, Privacy*, ARS TECHNICA, http://arstechnica.com/old/content/2008/03/ny-bill-would-police-intersection-of-online-ads-privacy.ars (last visited May 12, 2009).

356. Hotaling, *supra* note 13, at 563; Personal Data Privacy and Security Act, S. 495, 110th Cong. (2007), *available at* http://www.govtrack.us/congress/bill.xpd?bill=s110-495&tab=summary.

357. Personal Data Privacy and Security Act, S. 495, 110th Cong. (2007), *available at* http://www.govtrack.us/congress/bill.xpd?bill=s110-495&tab=summary.

> conduct risk assessments of potential security breaches; (3) adopt risk management and control policies and procedures; (4) ensure employee training and supervision for implementation of data security programs; and (5) undertake vulnerability testing and monitoring of personal data privacy and security programs.[358]

The act also would have enacted a federal data breach notification requirement.[359]

Compared to other proposals, the act would have done more to address the storage, maintenance, and use of consumer information than to address issues of notice and consent.[360] It was far more explicit than the FTC's principles in elaborating on the kinds of security risks that a covered entity must consider, audit, and avoid.[361] The bill, however, never reached the floor of the full senate.[362]

4. COPPA

One observer has suggested that the Child Online Privacy Protection Act, which gives parents significant control over advertisers' use of data relating to children, would be a suitable template for expansion.[363] Expanding COPPA to protect all individuals (rather than just children) "would command consent from the individual whose information should be collected."[364] This approach would legislatively mandate the "opt-in" approach and give consumers the chance to view the data profilers collect.[365] And, it would affirm that consent to profiling must come from the profiled consumer, and give the consumer the right to revoke that consent.[366]

5. Draft 2010 House Legislation

United States Representatives Rick Boucher and Cliff Stearns recently announced a new draft bill to address the privacy concerns inherent in the collection of information about individuals.[367] This law

---

358. *Id.*

359. *Id. See generally* Sprague & Ciocchetti, *supra* note 101, at 137-40.

360. *Id.*

361. *Cf.* PRINCIPLES, *supra* note 7, at 37.

362. Personal Data Privacy and Security Act, S. 495, 110th Cong. (2007), *available at* http://www.govtrack.us/congress/bill.xpd?bill=s110-495&tab=summary.

363. *Supra* Part II.D.; Hotaling, *supra* note 13, at 559-61.

364. *Id.* at 560.

365. *Id.*; *see* 15 U.S.C. § 6502(b)(1)(B) (2006) (giving parents the right to view collected data).

366. Hotaling, *supra* note 13, at 562.

367. Stephanie Clifford, *Consumer Groups Say Proposed Privacy Bill is Flawed,* N.Y. TIMES, May 5, 2010, at B3. Rick Boucher is a Democratic congressman from Virginia, and Cliff

"would be the first law that applies generally to businesses requiring privacy notice, particularly in the offline space."[368] In essence, the draft bill would require covered entities to disclose their data collection to consumers and obtain consent to the collection.[369] The bill presumes that consumers consent to the collection of most information if the covered entity has provided a compliant privacy policy and the consumer chooses not to opt out of the collection.[370] The bill also requires consumers to opt in to the collection of certain sensitive information.[371] And, the bill prohibits a covered entity from using information it has collected if a consumer withdraws consent.[372]

The draft bill also imposes accuracy and security requirements on covered entities.[373] It requires covered entities to maintain "appropriate administrative, technical, and physical safeguards that the [FTC] determines are necessary" to (1) "ensure the security, integrity, and confidentiality of such information; (2) "protect against anticipated threats or hazards to the security or integrity of such information;" (3) "protect against unauthorized access to and loss, misuse, alteration, or destruction of, such information;" and (4) "in the event of a security breach, determine the scope of the breach, make every reasonable attempt to prevent further unauthorized access to the affected covered information, and restore reasonable integrity to the affected covered information."[374] The failure to do so is treated as an "unfair and deceptive act or practice" in violation of the FTC Act.[375] The bill also vests enforcement authority in state attorneys general,[376] although it provides no private cause of action to

---

Stearns is a Republican congressman from Florida.

368. *Id.*

369. Website of U.S. Congressman Rick Boucher, Boucher, Stearns Release Discussion Draft of Privacy Legislation, http://www.boucher.house.gov/index.php?option=com_content&view=article&id=1957:boucher-stearns-release-discussion-draft-of-privacy-legislation-may-4-2010&catid=33:2010-press-releases&Itemid=41 (last visited May 8, 2010); STAFF OF H. SUBCOMM. ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET, 11TH CONG. DISCUSSION DRAFT: A BILL TO REQUIRE NOTICE AND CONSENT OF AN INDIVIDUAL PRIOR TO THE COLLECTION AND DISCLOSURE OF CERTAIN PERSONAL INFORMATION RELATING TO THAT INDIVIDUAL § 3(a)(1), *available at* http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf [hereinafter DRAFT BILL].

370. DRAFT BILL § 3(a)(3)

371. *Id.* at § 3(c).

372. *Id.* at § 3(a)(3)(A).

373. *Id.* at § 4.

374. *Id.* at § 4(b).

375. *Id.* at § 8(a)(1).

376. DRAFT BILL § 8(b). Attorneys general would enforce the terms of the draft bill solely

consumers who are harmed through the disclosure of their profile.[377] Finally, the bill sets an exclusive national standard and preempts state or municipal regulations that impose "requirements for the collection, use, or disclosure of covered information."[378]

6. Limitations of Existing Proposals

All of these proposals have significant merit and each addresses some problems associated with behavioral targeting. The proposals that deal with notification and consent, however, all have the potential to cause unintended harm to consumers.[379] As described previously, websites have come to rely on advertising to support their content. And, website operators are looking for ways to transition other forms of content–like television and newspapers–to the web, but struggle to fund the storage and distribution of this content.[380] One of the chief ways the Internet can make this innovative distribution model appealing to content producers is by allowing those distributors to market to consumers precisely. Behavioral advertising does this. Therefore, proposals that strengthen the consent requirement through opt-in or "do-not-track" methods risk destroying these business models. These proposals may force businesses to implement a "take it or leave it" approach requiring consumers to give their consent before taking advantage of a website's content;[381] targeted advertising is the only way businesses derive the necessary revenue from their customers. If businesses take the "take it or leave it" approach, these proposals aimed at consent will help very little. They will increase administrative burdens on businesses engaged in behavioral targeting without improving privacy for consumers, who, as a practical matter, will probably use the services anyway.[382]

Further, none of the existing proposals fully address the obstacles to enforcement of consumers' rights. While the notice and consent requirements do partially address the issue of data collection transparency, consumers may be left guessing as to what data

---

in federal district court. *Id.*

377. *Id.* § 9.

378. *Id.* § 10.

379. *See supra* Parts I.C and IV.A (explaining the benefits of behavioral targeting, and how certain regulations might interfere with these benefits).

380. *See supra* Part I.C and notes 178-190.

381. *See also* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 825-27 (2000) (discussing the interplay between consent requirements and "'take-it-or-leave-it' . . . data processing").

382. *See generally id.* at 823 (explaining why consumers cannot readily "exit" because "there is nowhere else to go").

profilers have actually collected, how they have used it, and whether they have reasonably safeguarded this data. While the FTC may deal with the most egregious violators, fairness requires that some compensation be available to victims of profilers that inappropriately use or disclose data.

B. Broaden, Mandate, and Audit

Therefore, I argue that none of the existing approaches, including the FTC's principles, adequately balance the protection of consumers' privacy interests with the potential benefits of behavioral targeting for consumers. Some proposals, because they focus on strengthening consent requirements, run the risk of unnecessarily destroying or seriously impeding even the most benign business models based on behavioral targeting. In addition, the existing approaches fail to give consumers information they need to make rational choices about whether to participate in behavioral targeting and fail to give regulators information required to enforce compliance. Indeed, consumers are in a poor position to use any authority to opt in or opt out of data collection because they lack information necessary to accurately gauge the risk of being harmed.

Thus, the FTC should (1) expand its self-regulatory principles to all significant profilers of consumer information, (2) enforce them as mandatory regulations, and (3) require organizations to periodically audit and publish their compliance with the regulations, reasonable information security practices, and privacy policies.

First, I urge the FTC to expand the scope of its self-regulatory principles to all significant profilers of consumer information. At present, the principles do not apply to profilers that collect consumer information for purposes other than advertising, nor do they apply to profilers who collect data on consumers exclusively for their own use.[383] As Part I.B demonstrated, the harm to consumers that can stem from behavioral targeting is not limited to the advertising context. Nor does the mere fact that a profiler does not share its profiled data mean that the data cannot be misused or inadequately safeguarded. Rather, the harms associated with behavioral targeting can occur any time a profiler compiles a database of consumer information. This change would also have a salutary effect in that profilers would all face the same regulations; there would be no benefit to a profiler in trying to characterize its business as being outside the boundaries of

383. *Supra* Part III.A.

the regulation.

Second, I urge the FTC to make the self-regulatory principles mandatory regulations.[384] As self-regulatory principles, the rules have the potential to cause a "race to the bottom" effect.[385] Profilers who voluntarily comply with the regulations may face an added burden and expense. This places them at a competitive disadvantage relative to profilers who choose not to comply with the self-regulatory principles.[386] Moreover, there is no reason to believe that consumers understand the self-regulatory principles or even know of their existence.[387] Therefore, they likely cannot select businesses based on their compliance with the principles. And, in many cases, profiling is completely invisible to the consumer, so the consumer cannot make an informed decision as a market participant. Under these circumstances, profilers that ignore the self-regulatory principles are placed in a position more favorable than the principles' adherents.[388]

Furthermore, the FTC's principles already provide protections for consumers that balance privacy protection against the needs of commerce and industry. They are the product of an extensive discussion among profilers, regulators, and consumer advocates.[389] In many ways, the burdens the FTC's principles impose overlap with the

---

384. *See* Ciochetti, *supra* note 123, at 11 n.39 (noting the importance of enforcement in protecting consumers' privacy).

385. *See* David Lazer & Viktor Mayer-Schönberger, *Governing Networks: Telecommunication Deregulation In Europe And The United States*, 27 BROOK. J. INT'L L. 819, 827 (2002) (describing the race to the bottom problem in state corporate regulation). The race to the bottom problem occurs when competitors choose an inferior lower-cost option even when they prefer a higher-cost option because they fear the higher-cost option will cause them to lose to the competition. *See id.*

386. *See* Ciocchetti, *supra* note 123, at 26-27 ("Under a self-regulatory regime, businesses have little incentive to protect privacy at the expense of profits.").

387. *See* Bob Tedeschi, *E-Commerce Report; Everybody Talks About Online Privacy, but Few Do Anything About It*, N.Y. TIMES, Jun. 3, 2002, at C6 ("E-Loan and Expedia began subjecting themselves to voluntary privacy audits by PricewaterhouseCoopers in 1999 and 2000. The audits have helped demonstrate that the companies' internal data-handling methods are consistent with their privacy policies, but they have not sparked much interest among competing companies."). While seal organizations, such as the Better Business Bureau, may be already playing a role in certifying that profilers comply with their own privacy policies and protect consumer data, E-Commerce/Click-Away, *Protecting Consumer Data*, NEWSDAY, Mar. 29, 1999, at C07, because participation in seal organization's program is necessarily voluntary, it cannot serve as an effective substitute for mandatory regulation.

388. *See* Tedeschi, *supra* note 387 (noting that Expedia's audits cost about $120,000 annually, but that there is "a surplus of consumer apathy when it comes to privacy"). It seems likely that consumers' apathy derives from their inability to discriminate among the privacy practices of the businesses they patronize, as well as the difficulty of assigning value to the differences.

389. *See* PRINCIPLES, *supra* note 7, at i-iv.

mandatory obligations that profilers face under the FTC Act.[390] Indeed, profilers that comply with the existing self-regulatory principles may already be in or near compliance, and, thus, will face little added burden if the principles become mandatory.

Third, and most importantly, the FTC should enact regulations requiring profilers to periodically audit their adherence to the principles, reasonable information security practices, and their published privacy policies. The regulations should require profilers to make the results publicly available.[391] Public companies in the United States are already required to periodically prepare audited financial statements to give shareholders and investors information about the companies' financial status.[392] This information allows shareholders, who would otherwise have no way to know whether officers of the company were acting in their best interests, to see a variety of metrics about the company's financial performance.[393] It also allows investors to make an informed decision about whether to purchase shares in such a corporation.[394] Under present law, the auditor must certify that the audited financial statements comply with generally accepted accounting principles.[395] Thus, the audited financial statements allow investors to make an informed decision about whether to invest in the

390. *See id.* at 20.

391. *See also* Center for Democracy and Technology, *Online Behavioral Advertising: Industry's Current Self-Regulatory Framework Is Necessary, but Still Insufficient on Its Own To Protect Consumers* (Dec. 9, 2009), http://www.cdt.org/policy/online-behavioral-advertising-industry's-current-self-regulatory-framework-necessary-still-in#3 (last visited Mar. 28, 2010) (recommending "compliance reviews" of behavioral advertisers to be conducted by "independent third parties"); PRIMER, *supra* note 145, at 5, 11 ("A behavioral targeter must conduct an independent audit of its operations for compliance with this law, and it must make the results of that audit public.").

392. *See* ALAN R. PALMITER, CORPORATIONS: EXAMPLES AND EXPLANATIONS 363-366 (5th ed. 2006); U.S. Securities and Exchange Comm'n, Form 10-K, http://www.sec.gov/answers/form10k.htm (last visited July 25, 2010) ("The annual report on Form 10-K provides a comprehensive overview of the company's business and financial condition and includes audited financial statements.").

393. Paul G. Mahoney, *Mandatory Disclosure as a Solution to Agency Problems*, 62 U. CHI. L. REV. 1047, 1085-86 (1995).

394. *Id.* at 1085. Mahoney notes that financial reporting serves both to aid in resolving the agency problem and to inform investors: In the context of ongoing reporting, two distinct conceptions of the function of financial reporting are possible. One might view financial reporting as principally a form of monitoring for the benefit of shareholders, creditors, and other interested parties. Alternatively, one might view accounting as a means of providing a comprehensive picture of a firm's performance that may enable investors to form a better judgment of the value of the firm and its securities. *Id.*

395. Theodor Baums & Kenneth E. Scott, *Taking Shareholder Protection Seriously? Corporate Governance in the United States and Germany*, 53 AM. J. COMP. L. 31, 45 (2005).

company.[396]

A privacy compliance audit could serve similar purposes. Since profilers' information handling practices are generally not known to consumers unless the profiler experiences a high-profile data breach, the audit could alert the FTC or other authorities to major transgressions. Of course, a routine audit requirement would also alert profilers to gaps in their own compliance, and allow profilers to proactively address them. In addition, the audit would allow consumers, consumer advocates, and the businesses that profilers serve to make informed decisions about which companies are the reliable companies with which to do business.[397] Indeed, the audits would give consumers the very information they need to determine the likelihood of harm occurring because of their participation in behavioral targeting, and, thus, the audits would vastly improve consumers' ability to gauge the risk associated with participation in behavioral targeting. And, over time, regulators could use this information to determine whether further regulation of behavioral targeting is needed. For most companies, a compliance audit could probably take place in conjunction with existing financial or information system audits, since these audits are common in public corporations and other large businesses.[398]

If the FTC were to enact these proposals, it would also partly address the problems associated with private enforcement of consumers' privacy rights. The audits would assist consumers in discovering organizations with noncompliant information security or management practices, and give them a starting point for investigation of suspected cases of harm. Thus, the organization's privacy policy and compliance audit would substantially narrow the information gap

396. Mahoney, *supra* note 393, at 1085.

397. Consequently, rather than encouraging a race to the bottom, the regulations would create an incentive system for compliance with the regulations. Although individual consumers would not likely assiduously investigate the audit results for individual profilers, profilers can reasonably expect that the media and consumer advocates will make use of this information, digest it, and relay it to consumers in a usable form.

398. *See* Victor Godinez, *Laws Stir Demand For Tech Specialists IT Auditors Build Systems to Track Data to Comply With Sarbanes-Oxley, Other Legislation*, DALLAS MORNING NEWS, July 25, 2004, at 5J (noting that the passage of the Sarbanes-Oxley act required companies to have better information technology controls, and that auditors verify these controls during their audits); *see also* Sarah E. Needleman, *Sarbanes-Oxley Creates Special Demand --- Need for Veteran IT Auditors Intensifies Amid Tightened Financial-Reporting Rules*, WALL ST. J., May 16, 2006, at B8 ("The need for IT auditors has intensified since most large and midsize publicly traded companies were required to become Sarbanes-Oxley-compliant for the first time in 2004, say recruiters. Most companies must prove compliance on an annual basis, and IT auditors help ensure Sarbanes-Oxley controls are operating effectively.").

that currently makes private civil enforcement actions difficult to bring. Even with the information gap thus narrowed, civil lawsuits may not truly be an effective way of promoting consumers' privacy interests.[399] Nevertheless, in other contexts, the existence of parallel regulatory and civil enforcement methods has ensured that there is some recourse for a consumer when the regulatory agency chooses not to act.[400]

V. CONCLUSION

When I talk to my non-lawyer friends and family, I love to tell them about the law that I know they will strongly disagree with. I remember telling my mother about *Moore v. Regents of the University of California*,[401] in which the California Supreme Court concluded that the plaintiff, John Moore, did not actually own the cells of his body. The defendants had used Moore's cells to derive a valuable stem cell line.[402] The defendants did not share any of the profits with Moore, or even inform him that they had used his cells to grow a product that they were selling commercially.[403] The majority opinion concluded that Moore had no property interest in the cells that University of California researchers took from his body.[404] After telling my mother about the case, she exclaimed, "Well, *I* own *my* body!"

The collection of consumer information presents an analogous disconnect between legal doctrine and general societal understanding about ownership. It surprises me that in all of the legal discussion of

399. *See* Sprague & Ciocchetti, *supra* note 101, at 101 ("For victims of identity theft, the principal obstacle for seeking damages through the courts has been the lack of actual damages suffered - the threat of harm resulting from identity theft is insufficient."). However, the draft 2010 legislation discussed in part IV.A.5 also allows state attorneys general to enforce the bill's provisions in federal court. I heartily endorse this as a sensible addition to privacy legislation, because it gives consumers another, perhaps more accessible advocate for their privacy rights. Another approach to making the civil litigation system more effective is to give consumers a clear private right of action accompanied by "liquidated damages, attorney fees, and costs for successful plaintiffs." PRIMER, *supra* note 145, at 10.

400. *See* Jay Cook, Editorial, *Tort Reform: Corporations Put Profit Before Safety*, ATLANTA J.-CONST., Sept. 18, 2007, at 11A (contending that the Food and Drug Administration was incapable of protecting consumers from drugmakers, and that Americans injured must turn to the court system); 15 U.S.C. §§ 1681n, 1681o, and 1681s (creating parallel administrative and private civil enforcement remedies under the Fair Credit Reporting Act).

401. Moore v. Regents of the Univ. of California, 793 P.2d 479 (Cal. 1990), *cert. denied*, 499 U.S. 936 (1991).

402. *Id.* at 481.

403. *Id.* at 482.

404. *See id.* at 493.

consumer information, we have not fully resolved the question of who, if anyone, ought to *own* information about consumers and their activities.[405] If property is, as our property professors teach us, largely a way of rendering social conventions about the right to exclusively possess, transfer, and dispose of beneficial objects and intangibles into a workable legal framework,[406] I think that the social convention would be to regard a consumer's information as that consumer's property. Indeed, I expect my mother would say, "Well, *I* own *my* information!" People refer to consumer information relating to them using the word "my," and I think this is powerfully telling. When we, as lawyers, try to figure out how to protect consumer data, we have to resort to a complicated web of laws dealing with privacy, wiretaps, computer fraud, unjust enrichment, and hacking to analyze what would seem to nonlawyers–like my mother–to be a simple question of ownership.[407]

It is likely too late to suggest that consumers actually do *own* their information,[408] and that we should, therefore, analyze the rights of profilers based on a concept of a license to use the data. Nonetheless, the best solutions in this area must accommodate the concept that consumers think of personal information as their property, and their privacy and ownership expectations reflect this. This premise respects the popular social construction of ownership while still allowing behavioral advertisers and other users of behavioral targeting to aggregate and transform consumer information into an economically valuable and useful product.

The FTC's self-regulatory principles, enhanced as I have described above, are a workable balance. They protect consumers' interest in knowing how their information is used. They give consumers assurances that it will be handled according to their expectations. They give them the information they need to seek

---

405. *See generally* SOLOVE, *supra* note 123, at 638-39 (quoting LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999)); Julie E. Cohen, *Examined Lives: Informational Privacy and The Subject as Object*, 52 STAN. L. REV. 1373, 1377-1391 (2000).

406. *But see* Cohen, *supra* note 405, at 1379-80 (noting how "property language both describes *and determines* our experience of reality") (emphasis added).

407. *But see* SOLOVE, *supra* note 123, at 639-40 (quoting Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN L. REV. 1125, 1137-47 (2000) (suggesting property rights are not sufficient to safeguard privacy)).

408. *But see New Rules For Big Data*, THE ECONOMIST, Feb. 27, 2010 (suggesting that "privacy rules lean towards treating personal information as a property right"). "A reasonable presumption might be that the trail of data that an individual leaves behind and that can be traced to him, from clicks on search engines to book-buying preferences, belong to that individual, not the entity that collected it." *Id.*

redress when their expectations are violated. They allow the FTC to act on consumers' behalf when the FTC's principles are not followed. They allow profilers to continue using a critical tool for generating business-sustaining revenue. This may be the closest we can practically come to actually living up to consumer's expectations about how their data will be used without prohibiting or severely restricting consumer profiling.

* * *