WHO'S FOLLOWING YOU: THE FEDERAL TRADE COMMISSION'S PROPOSED "DO NOT TRACK" FRAMEWORK AND ONLINE BEHAVIORAL ADVERTISING

Timothy J. Shrake II*

I. INTRODUCTION

You do not see it when it occurs, but you definitely see the results. Imagine you are an avid sports fan. You search your team's name to see the latest news. You constantly visit ESPN to check the scores. You buy merchandise off of Amazon.com. You list your favorite teams on Facebook. Chances are that you will start seeing advertisements based on your interest as a sports fan. These advertisements are directly tailored to your use of the internet on your computer, and this is online behavioral advertising.[1] In simple terms, online behavioral advertising takes information individuals convey over the internet through search engine queries, web pages visited, and content viewed, and uses this information to tailor specific advertisements to that individual.[2]

In the 21st century, technology progresses at an exponential rate. Fifteen years ago, only two graduate students could tell you what Google was.[3] With technological innovations fueling the internet's expansion and complexity, new issues concerning internet regulations, consumer rights, and privacy, constantly come to the forefront. These issues must be balanced, and a key goal of this commentary is to shed light on this question—what is the best way to protect consumer privacy while at the same time advancing the benefits of the internet and technological innovation.

This comment will explain the current backdrop of online behavioral advertising, examine recent developments in the law, and analyze proposed mechanisms for regulating online behavioral advertising. Section II will

---

* Timothy J. Shrake II is a third-year law student expecting his J.D. from Southern Illinois University School of Law in May 2012. The author would like to thank Professor Tracie Porter for her guidance and advice in writing this Comment. He would also like thank his parents, Tim and Jennifer Shrake, for their never-ending support.

1. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVER. 2 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.
2. *Id.*
3. *Corporate Information*, Google, http://www.google.com/corporate/ (last visited Mar. 26, 2011).

give a more detailed explanation of online behavioral advertising while also discussing the Federal Trade Commission's (FTC) 2009 self-regulatory framework. Section III will examine the FTC's most recent proposal, 'Do Not Track,' as it primarily relates to online behavioral advertising; as well as provide a brief overview discussing the current state of self-regulation. Section IV will analyze the 'Do Not Track' proposal, the realities of regulation, and also internet privacy expectations while taking into consideration the public viewpoint regarding online behavioral advertising. Finally, the comment will discuss possible alternatives to 'Do Not Track' in light of various opinions from governmental and academic sources.

II. BACKGROUND

The internet phenomenon has bred the practice of online behavioral advertising. As noted above, online behavioral advertising "involves the tracking of consumers' online activities in order to deliver tailored advertising" to consumers.[4] Online behavioral advertising involves two overarching steps: 1) following an individual's actions from an internet capable device[5]; and 2) tailoring advertisements for those individuals based on their actions.[6] There are primarily two types of entities that engage in online behavioral advertising: network advertisers and individual websites.[7] Network advertisers are the companies which choose and convey the advertisements an individual sees when they visit a specific website.[8] These network advertisers maintain vast networks that can consist of hundreds, thousands, or even tens of thousands of individual websites.[9] Network advertisers then use individual websites to both collect data as a consumer travels across the various websites in an advertising network and also convey targeted advertisements.[10] To gain a better idea of these network advertisers, it is useful to know that almost all major search engines own advertising networks, with Google owning the largest market share.[11] In order to demonstrate how online behavioral advertising works

4. F.T.C., SELF-REGULATORY, *supra* note 1, at 2.
5. An important distinction to remember is that online behavioral advertising is not advertising to an individual *per se*; rather, online behavioral advertising is advertising to a specific internet capable device. It just so happens that most people use the same internet capable device day in and day out, and that due to this fact, online behavioral advertising relates to the potential interest of that individual.
6. Joseph Turow, et al., Americans Reject Tailored Advertising: and Three Activities that Enable It 3 (Sept. 29, 2009), *available at* http://ssrn.com/abstract=1478214.
7. *Id*. at 5.
8. F.T.C., SELF-REGULATORY, *supra* note 1, at 3.
9. Turow, *supra* note 6, at 5.
10. F.T.C., SELF-REGULATORY, *supra* note 1, at 3.
11. Turow, *supra* note 6, at 5-6.

across an advertising network, imagine you want to take a vacation to Bora Bora and you visit a website to research the island. The next day, while you visit a news website, you may see an advertisement for Bora Bora if the websites are in the same advertising network.

Online behavioral advertising occurs invisibly, without an individual knowing that certain information is being transmitted. Websites and network advertisers typically gain this information through the use of "cookies."[12] A cookie "is a small text file that a website's server places on a computer's web browser."[13] The cookie then sends information to the server about the user's internet activities on that website.[14] Network advertisers then compile this information to create profiles[15] of computer users.[16] These nameless profiles begin to paint a picture of an individual's life for advertisers, potentially revealing information such as one's gender, interest, lifestyle, and personality.[17] For example, someone who visits different websites in an advertising network featuring hair-loss, golf, world traveling, and retirement homes would have a profile which certain advertisers would find useful.[18] The idea which fuels online behavioral advertising is that targeted advertisements result in increased sales. As a result, these companies tailor and deliver advertisements based upon data collected from an individual's internet usage as that individual surfs across the various websites in an advertising network.

Turning towards consumer protection, the FTC maintains a general goal in the privacy arena: "to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace."[19] One must remember that this broad goal goes beyond protecting individuals on the internet, and touches many facets of consumerism. In promoting this goal, the FTC has embraced a flexible approach and has primarily used two models to further consumer

---

12. F.T.C., SELF-REGULATORY, *supra* note 1, at 2 n.3.
13. *Id.*
14. *Id*. at 2.
15. Once again it is important to remember the distinction between tracking an individual and tracking a computer an individual uses. Therefore, this method of advertising is not saying "Jon Smith likes Ford Mustangs;" rather it is saying "this computer user likes Ford Mustangs." However, personal identifying information can be tied to these profiles. *See, e.g., In re* Doubleclick, 154 F.Supp.2d 497 (S.D.N.Y. 2001).
16. Turow, *supra* note 6, at 6.
17. *Id.* at 6-7.
18. It should be noted that because a named individual does not have a profile, inferences are used to target advertisements. While most would think the advertisement given above refers to an older male, the internet user could just have easily been a balding 40 year old, who enjoys golf, who is getting ready to find a retirement home for his parents.
19. FED. TRADE COMM'N., PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUS. AND POLICYMAKERS iii (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

protection: 1) the "notice-and-choice model" and 2) the "harm-based model." These models refer to two regulatory schemes/ideologies the FTC embraces in trying to protect consumers. The "notice-and-choice model" refers to providing explanatory information to consumers. This model "encourages companies to develop privacy notices describing their information collection and use practices to consumers, so that consumers can make informed choices."[20] The "harm-based model" focuses on harms done to consumers and looks to protect them from risks dealing with "physical security, economic injury, and unwanted intrusions" into their daily activities.[21]

The "notice-and-choice model" possesses four main components: 1) companies should provide notice of the information they collect and their use of it; 2) consumers should have a choice about how information collected may be used; 3) "consumers should have access to the data collected about them;" and 4) companies should safeguard the data collected from consumers.[22]

As it pertains to the internet, the "notice-and-choice model" did not fully protect consumers in this unregulated and ever advancing field. As a result, the FTC started focusing, and taking action, on specific consumer harms as a means of protecting and addressing consumer privacy concerns.[23]

These models, however, are not without their flaws. The FTC has questioned whether these models can effectively keep pace with innovative technologies that allow companies to collect and use consumers' information in ever changing ways.[24] The "notice-and-choice model" has resulted in an immense amount of near incomprehensible legalese, such as privacy policies, which the typical individual merely clicks through.[25] Even if a typical consumer reads these privacy policies, many do not understand the terms to which they are consenting.[26] Furthermore, these privacy policies focus more on limiting a companies' liability rather than disclosing how a consumer's online information will be used.[27]

---

20. *Id.*
21. *Id*.
22. *Id*. at 7.
23. *Id*. at 9.
24. *Id*. at 19.
25. *Id*. at iii.
26. *See* Felicia Williams, *Internet Privacy Policies: A Complex Index for Measuring Compliance to the Fair Information Principles* 17-18 (2006), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf This report examined privacy policies of Fortune 500 companies. The report found that "only one percent of the privacy policies were understandable for those with a high school education or less and thirty percent required a post-graduate education to be fully understood." *Id.*
27. F.T.C., PROTECTING CONSUMER PRIVACY, *supra* note 19, at 19.

While the "harm-based model" takes action against companies, its limited focus of responding to specific harms, such as physical security, economic injury, and unwarranted intrusions into consumers' lives, leaves unchecked issues of reputational harm and tracking/monitoring fears.[28] The peculiarities of the internet make application of the harm-based model even more difficult. In terms of general internet privacy enforcement, the FTC relies on Section 45 of the Federal Trade Commission Act.[29] Section 45 states "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[30] Given that website and network advertisers may currently track your movements on the internet, the FTC's main instruments in privacy enforcement[31] are companies' privacy policies.[32] If a company uses your information as otherwise stated, then they may encounter charges of deception, but as earlier noted, companies use these privacy policies as a way to limit their liability.[33]

In February 2009, the FTC took a closer look at online behavioral advertising and published a staff report entitled, *Self-Regulatory Principles for Online Behavioral Advertising*.[34] As the title notes, the FTC took a self-regulatory approach to online behavioral advertising rather than trying to enact legislation. The report provides four overarching provisions in their self-regulatory system: 1) Transparency and Consumer Control; 2) Reasonable Security, and Limited Data Retention, for Consumer Data; 3) Affirmative Express Consent for Material Changes to Existing Privacy Promises; and 4) Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising.[35]

The first provision, Transparency and Consumer Control, looks to those websites which collect consumer data and focuses on providing a "clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interest; and (2) consumers can choose whether or not to have their information collected for such purpose."[36] The next provision,

---

28. *Id*. at 20.
29. Federal Trade Commission Act of 1914, 15 U.S.C. § 45 (2006).
30. *Id*.
31. Congress has enacted specific regulatory schemes for areas such as finance, but not for internet tracking.
32. Google/Doubleclick, File 071-0170 16, 2007 WL 4624893 (F.T.C. Dec. 20, 2007) (Harbour, dissenting).
33. *Id*.
34. F.T.C., SELF-REGULATORY, *supra* note 1.
35. *Id*. at 2.
36. *Id*. at 46.

Reasonable Security and Limited Data Retention, adheres to the idea that companies should keep an individual's data "only as long as necessary to fulfill legitimate business or law enforcement needs," while at the same time protecting that individual's data.[37] The third provision, Affirmative Express Consent for Material Changes to Existing Privacy Promises, focuses on the idea that before a business can use your previously collected data in a materially different manner than a previous privacy policy stated, the business should obtain the express consent from individuals before using their information under the new privacy policy.[38] Finally, the Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising provision relates to the core idea that "[c]ompanies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising."[39]

The 2009 self-regulatory principles for online behavioral advertising did not command a change in the landscape. A 2010 report by the FTC stated "[i]ndustry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."[40] Companies have an incentive, though, to limit self-regulation. The more companies self-regulate, the likelihood of decreased profits from behavioral advertising increases. Furthermore, the 2010 report found that "while many companies disclose their practices, a smaller number actually offer consumers the ability to control these practices."[41] In other words, many websites tell you what they will do with your information, but provide no means to limit how they use your information.

III. RECENT DEVELOPMENTS

On December 2, 2010, the FTC issued a proposal for the regulation of consumer privacy issues, among them online behavioral advertising.[42] This proposal, *Protecting Consumer Privacy in an Era of Rapid Change*,[43] would broadly apply to both online and offline commercial entities that "collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer, or device."[44] This

37 *Id.* at 47.
38. *Id.* at 47.
39. *Id.* at 47.
40. F.T.C., PROTECTING CONSUMER PRIVACY, *supra* note 19, at iii.
41. *Id.* at 19.
42. *Id*.
43. *Id.*
44. *Id.* at v.

report recognized some of the defects in the 2009 report on self-regulation in the world of online behavioral advertising. The FTC's proposed framework has three main principles: 1) a greater promotion of consumer privacy throughout the company; 2) simpler consumer choices; and 3) an increase in transparency of companies' data practices.[45] Under the principle of simplifying consumer choices, the FTC addressed online behavioral advertising. As a result, the other principles will be only briefly discussed.

The first principle of promoting consumer privacy throughout a company has also been referred to as the Privacy by Design approach.[46] This goes to the simple idea of augmenting privacy protection in everyday business practices by "providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy."[47]

The second principle, simplifying consumer choice, encompasses the proposed mechanism for online behavioral advertising—'Do Not Track.'[48] The framework of simplifying choice advocates that companies provide choices to consumers regarding "whether to allow the collection and use of data regarding their online searching and browsing activities."[49] In general, the report states that the efforts to implement consumer choice on an industry-wide basis have fallen short.[50] These efforts to implement consumer choice fell under a previous self-regulatory framework.

Next, even though some mechanisms exist to allow consumers a choice in the matter of online behavioral advertising, consumers are often unaware of them.[51] While some consumers may be aware of existing mechanisms, these mechanisms do not necessarily clarify the extent or scope of the choice being offered.[52] For example, some of the existing mechanisms do not make clear whether one is choosing not to be tracked or merely choosing to be tracked but not be the recipient of targeted advertising.[53] Finally, the average individual will likely not be aware of the limitations of existing control mechanisms.[54] Without a user friendly or simplistic method for delivering choices to consumers, many are bound to

---

45. *Id.* at v-vii.
46. *Id.* at v.
47. *Id.*
48. *Id.* at 63.
49. *Id.* at vii.
50. *Id.* at 64.
51. *Id.* at 64-65.
52. *Id.* at 65.
53. *Id.*
54. *Id.*

get lost in the technical minutia of the trade. For instance, an individual might believe they have opted out of tracking by blocking third party cookies on their web browsers; however, they could still be tracked through a variety of other means, such as Flash cookies.[55]

In light of the shortcomings under the current self-regulatory scheme, the FTC supports and advances "a more uniform and comprehensive consumer choice mechanism for online behavioral advertising," referred to as 'Do Not Track.'[56] In terms of a means to carry out the end of a uniform and comprehensive consumer choice mechanism, the FTC recommends "placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements."[57] With the promulgation of the 2010 report, the FTC recognizes the shortcomings of an unenforceable, self-regulatory scheme. Therefore, in order for 'Do Not Track' to be effective, either Congressional legislations or "robust, enforceable self regulation" would be needed.[58]

A significant rationale underlying 'Do Not Track' is providing a mechanism that would "ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis," and that such choices would not be temporary or deleted whenever individuals erase their cookies.[59] This speaks to providing comprehensive coverage so that consumers have an easy, systematic way to tell the plethora of websites and network advertisers engaged in behavioral advertising that they do not want to be tracked.

The staff report mentions five important issues about the 'Do Not Track' mechanism.[60] Before noting these issues, it should be mentioned that the FTC relates these five issues rather broadly without much justification for its statements.[61] As a result, these issues are merely listed, and many of them will be discussed in Section IV. The staff report states:

> First, any such mechanism should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertising that many consumers value.
>
> Second, such a mechanism should be different from the Do Not Call program in that it should not require a "Registry" of unique

55. *Id.* at 65-66.
56. *Id.* at 66.
57. *Id.*
58. *Id.*
59. *Id.* at 66-67.
60. *Id.* at 67-69.
61. *Id.*

> identifiers . . . Commission staff recommends a browser-based mechanism through which consumers could make persistent choices.
>
> Third, some companies currently offer consumers a choice between opting out of online behavioral advertising altogether or affirmatively choosing the types of advertising they receive . . . at the roundtables,[62] . . . the panelist noted that, when given this option, rather than opting out of advertising entirely, consumers tend to choose to receive some types of advertising.
>
> […]
>
> Fourth, it is imperative that any universal choice mechanism be understandable and simple. In addition to being easy to find and use, such a mechanism should make it clear to consumers exactly what they are choosing and if there are limitations to that choice.[63]

Finally, while the staff has suggested general mechanics for a standardized choice mechanism, the FTC wants feedback for ideas, as well as the extent into mobile applications.[64]

IV. ANALYSIS

The analysis will first cover the actual need for regulation, including a 'Do Not Track' mechanism, and whether a governmental or self-regulatory framework should lead the way. Then, the analysis will examine the benefits and drawbacks of 'Do Not Track' as currently proposed. Next, internet privacy expectations and the public viewpoint concerning online behavioral advertising will be discussed. Finally, the analysis will look into alternatives to 'Do Not Track' and make a proposal in light of the FTC's, and others,' viewpoints and commentaries.

A. The Necessity of Do Not Track and Self-Regulation v. Governmental Regulation

The necessity of 'Do Not Track' emanates from the rapid growth of the internet and the need to ensure individual privacy rights. With the ever-changing landscape of the internet, regulation has fallen behind. By the end of 2010, the FTC recognized the failure of their 2009 report entitled *Self-*

---

62. The F.T.C. had roundtable discussions to gain feedback.
63. F.T.C., PROTECTING CONSUMER PRIVACY, *supra* note 19, at 67-68.
64. *Id*. at 68-69.

Regulatory Principles for Online Behavioral Advertising.[65] In December of 2010, the FTC stated, "industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."[66] While the FTC has not discarded the future for self-regulation, an inherent conflict poses serious questions about an effective self-regulatory scheme. This inherent conflict stems from the obvious difference between the financial interests of network advertisers and web-based companies and the privacy interests of many consumers. Network advertisers and web-based companies will not enact polices which financially hurt their businesses, especially if a practice proves to be financially beneficial. These entities have purposefully gathered information about internet users in order to try and increase profits. However, the gain of the almighty dollar in a largely unregulated field does not command the issue. Public perception, negative media exposure, competition, and pressure from the FTC act as countervailing forces.

With the three major internet browsers (Internet Explorer, Mozilla Firefox, and Google Chrome) increasing the level of anti-tracking technologies in the latest version of their browsers, one commentator asks whether the FTC's statement that self-regulation has been too slow is sound.[67] In the upcoming versions of the three major browsers, one will see that they incorporate anti-tracking technologies.[68]

Turning towards the necessity of 'Do Not Track,' while the three largest browsers have begun to take initiative, a need still exists for a 'Do Not Track' mechanism. This need comes from three current shortcomings: prominence, simplicity, and enforcement. Prominence relates to the fact that many of these anti-tracking features are shrouded within the options of a web-browser. Simplicity refers to the technical language used to describe the effects of anti-tracking mechanisms and how the average internet user may be unfamiliar with these terms. Finally, enforcement goes to the legal inability of the government or a private party to bring suit against a company which does not adhere to a consumer's anti-tracking wishes. As will be discussed in greater detail below, the most likely cause of action the government or a private party currently has is a breach of contract claim coming from a company's own privacy agreement.

---

65. *Id.* at iii.
66. *Id.*
67. Daniel Rockey, *Surveillance: Will the FTC's 'Do Not Track' Proposal Spell the End of Free Internet Content*, *in* BNA: PRIVACY AND SECURITY LAW REPORT (Jan. 31, 2011), *available at* http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=19151996&vname=pvlrnotallissues&fn=19151996&jd=a0c6d7z0m8&split=0.
68. *Id.*

While the three main web browsers have begun to break down technical terms and translate this information in an understandable way to the average internet user, more can be done. For a 'Do Not Track' mechanism to achieve its overarching goal, these mechanisms must become more prominent. Internet customs have destroyed traditional conspicuous language. With a paper contract, bolded font and capitalized letters readily mark conspicuous language. However, internet customs have minimized the functionality of these traditional methods of prominence. Pressed with an abundance of lengthy agreements shrouded in legalese, a typical consumer likely clicks through these agreements without ever deciphering what exactly they agreed to and how their information may or may not be used. Furthermore, while the internet has a near infinite number of uses, a significant amount of time spent on the internet is used for leisure activities.[69] Given this recreational component, a hypothesis exists that individuals do not understand the importance of many online agreements; as a result, they merely click through the agreements. One must also keep in mind the nature of many online agreements. On the World Wide Web, many agreements fall under the category of Terms and Conditions of Use (sites such as iTunes, Facebook, Amazon, etc). Outside of the internet context, however, many signed agreements deal with larger issues such as the purchase of a house or a car. As a result, people may be less inclined to pay full attention to internet agreements. Additionally, the ease of use of the internet adds to the need for simplicity. With the internet, all one really needs is the ability to read, type, and click a mouse. This aspect of simple functionality enables individuals to readily use the internet; however, when confronted with legal jargon, many will not understand the full extent of their agreement. Consequently, this ease of use coupled with the recreational component begs the question of how many individuals merely click through (and do not understand) an agreement in order to reach the goal of their internet use. This point goes to the idea of both simplicity and prominence. Given that people of various backgrounds and education use the internet, any type of 'Do Not Track' mechanism must be both simple to understand and prominent. If it is too complicated, individuals will fail to understand the technical language used to explain what 'Do Not Track' will do, and if it is not prominent, they might even fail to recognize the existence of such a mechanism. Due to what has been referred to as internet customs, a 'Do Not Track' mechanism must both distinguish itself from other typical internet notices or agreements and be expressed simply.

---

69. For example, Google released a report in 2010 that Facebook.com was the most visited site. Bianca Bosker, *Google Ranks Top 13 Most Visited Sites on the Web*, HUFFINGTON POST (May 28, 2010), http://www.huffingtonpost.com/2010/05/28/most-visited-sites-2010-g_n_593139.html#s94481&title=1_Facebookcom.

Focusing on the self-regulatory framework, one must keep in mind that while Microsoft, Mozilla, and Google have begun to increase anti-tracking measures, two of these companies (Microsoft and Google) possess strong incentives to restrict their helpfulness. Both Microsoft and Google own gigantic network advertisers; as a result, any restrictions these companies place on their browsers could have a negative effect on their own profits. For example, in an online tutorial offered when one downloads Google Chrome, behavioral advertising is cast in a favorable light.[70] The tutorial states "[c]ollecting real-world aggregate data and feedback from users can really help improve products and the user experience," and that "with cookies, a website you frequently visit is able to remember contents of your shopping cart, keep you logged in, and deliver a more useful, personalized experience based on your previous visits."[71] The tutorial on Google Chrome does mention the balance between privacy and efficiency, and that an individual can manage browsing cookies if they do not want websites collecting and remembering their online information.[72] However, this information does not possess the same positive spin as the information relating to the "benefits" of being tracked. Furthermore, given the discussion of how people likely click through notices, information relating to privacy and tracking cookies comes on page thirty-seven of the tutorial, making it less likely that Google Chrome customers actually read this material. While no statistics exist to see how many people read through this tutorial when they download Google Chrome, it is reasonable to ask if most merely skim through or even look at it at all.

One must remember that individual websites can partake in online behavioral advertising as well. For example, a Facebook executive stated "there is nothing controversial" about using the information from member profiles and wall postings to create targeted advertising for them.[73] While Facebook starts a tangential discussion about whether members have some sort of a privacy right,[74] the fact remains that using specific information to formulate ads may be controversial because a company accesses personal information for advertising purposes.[75]

---

70. Min Li Chan et al., *20 Things I Learned About Browsers & the Web*, GOOGLE CHROME, http://www.20thingsilearned.com/home (last visited Apr. 27, 2011).
71. *Id*.
72. *Id.*
73. Laurie Sullivan, *Facebook's Could be Demand-Gen Dollar Machine*, MEDIAPOST (Aug. 14, 2009), *available at* http://www.mediapost.com/publications/article/111629/.
74. This topic will be briefly discussed later in the comment under an individual's expectation of privacy.
75. For example, a Facebook user who posts her gender as female, her relationship status as single, and her age as 24 may see an ad to "Meet Single Dads in Your Area." To say this ad is not

Going to the heart of the issue, with just a self-regulatory approach, companies will inevitably lag behind in light of technological progression. Everyday programmers design new software, and the complexity and constant innovation of the internet will ensure the creation of new ways to track consumers and gain information. Granted, in terms of lagging behind, governmental regulation would also not match technological progression. Even so, governmental regulation would not have the countervailing force of profits holding them back from implementing a regulatory framework.

The self-regulatory approach also has enforcement issues. The main questions of 'Do Not Track' hinge not on the means to protect individuals. Instead, the question is one of enforcement. The FTC proposal states that the 'Do Not Track' mechanism can be "accomplished by legislation or potentially through robust, enforceable self-regulation."[76] This basic proposal does not reach the heart of the issue; instead, the crux and effectiveness of 'Do Not Track' centers on "an enforceable requirement that sites honor those choices."[77] As of right now, the FTC relies on traditional Section 5 authority to protect consumer's privacy rights on the internet.[78] This means that the FTC is pretty much restricted to enforcing companies' privacy policies.[79] In other words, the FTC can only go after a company for breaching their own privacy policy. However, these privacy policies are used to limit liability, and rarely will a company shoot themselves in the foot.

Given the legal status of online behavioral advertising, even if a browser has a 'Do Not Track' feature, network advertisers and individual websites do not have to heed this request.[80] Furthermore, "[u]nder current law, many companies are not required to provide—and do not currently provide—choice to consumers."[81] For example, Mozilla has its own 'Do Not Track' function which individuals may use to limit the information websites can ascertain from your browsing behavior.[82] However, even if someone decides to use Mozilla's 'Do Not Track' function, this does not mean websites must obey your request. Without legislation, abiding by a request to limit tracking information is purely voluntary.[83]

---

controversial gets off the subject of this paper, but people may find similar advertisements unpleasant.

76. F.T.C., PROTECTING CONSUMER PRIVACY, *supra* note 19, at 66.
77. *Id.*
78. Google/Doubleclick, No. 071-0170-16, 2007 WL 4624893 (F.T.C. Dec. 20, 2007) (Harbour, dissenting).
79. *Id.*
80. *How do I turn on the Do-not-track feature?*, MOZILLA FIREFOX, http://support.mozilla.com/en-US/kb/how-do-i-turn-do-not-track-feature?redirectlocale=en-US&redirectslug=how-do-i-stop-websites-tracking-me (last visited Oct. 23, 2011).
81. F.T.C., PROTECTING CONSUMER PRIVACY, *supra* note 19, at 53.
82. *How do I turn on the Do-not-track feature?*, *supra* note 80.
83. *Id.*

The most important provision of a 'Do Not Track' mechanism relates to enforcement and the subsequent ability of the FTC to put into effect consumers' wishes regarding tracking. Without such a provision, a form of internet piracy could potentially occur. Therefore, enforcement is one of the most recognizable problems with self-regulation. As noted above, in a self-regulatory framework the FTC could only protect consumers if a company violated their own privacy agreement, and "violations" of consumers' wishes would not necessarily matter because the companies themselves would be the ones enforcing consumers' wishes.

Whatever regulatory scheme is decided upon, whether it is robust self-regulation or governmental regulation, the anti-tracking mechanism must be (1) unique and prominent so that people do not merely skim over it; (2) simple so that the average internet user may understand its purpose and make an informed choice; and (3) enforceable so that individual companies do not abuse consumers' wishes and consequently gain a slight advantage relative to other competing companies.

B. The Benefits and Drawbacks of 'Do Not Track'

If online behavioral advertising did not have any benefits, no one would do it. The practice benefits both companies and some consumers. The practice benefits companies most notably by giving them greater revenue. A study by Howard Beales, the former Director of the FTC's Consumer Protection Bureau, found that behavioral advertising "is more than twice as effective at converting users who click on ads into buyers[84] . . . and that the weighted average cost per thousand ad impressions (CPM) for behaviorally targeted ads was $4.12, as opposed to $1.98 for run-of-network advertising."[85] The practice can also be positive and negative for consumers. Online behavioral advertising benefits some consumers by giving them the ads they want to see rather than irrelevant space fillers. It has an unfavorable aspect though. As will be noted in further detail below, many people do not like the thought of their online activities being tracked, and some might not like the generated advertisements that correlate to their online activity.

One argument against 'Do Not Track' states that this proposal would "undermine[] the implicit bargain which drives the internet and makes available to consumers vast amounts of information, seamlessly and without out-of-pocket cost to the consumer."[86] This argument posed by Daniel Rockey sees an implicit exchange of value between individuals and

84. Rockey, *supra* note 67. (6.8% conversion versus 2.8% conversion for regular ads).
85. *Id*.
86. *Id.*

internet content providers.[87] The idea of an implicit exchange of value seems to derive from a premise that nothing is truly free. Rockey's argument follows that "the content provider agrees to make content available to the consumer in exchange for the consumer's agreement to submit or display other ads."[88] To put this argument in another light, think of your local newspaper. Your local newspaper gains revenue from primarily two sources: 1) subscriptions and 2) sales from advertisements. The advertisements taken out in your newspaper are not keyed to your interest; they are generic. If a particular advertisement in the newspaper is particularly relevant, it is mere happenstance. Examining web-based content, many sources offer free information. Offering free information has a cost, whether one talks about it in terms of money or time. To offset this cost, many companies look for income from advertisements.[89] Online behavioral advertising offers targeted advertisements to produce greater revenue. The argument goes further by suggesting that generic advertisements may not generate sufficient revenue to ensure the continuance of free content; whereas online behavioral advertising results in the continuance of valuable, free content.[90]

Both the FTC and other commentators, such as Daniel Rockey, understand the benefits of online behavioral advertising. The FTC expressly stated in its 'Do Not Track' proposal: "[f]irst, any such mechanism should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertising that many consumers value."[91] If the premise is true that online behavioral advertising helps proliferate free online content, then hindering this source of revenue could decrease the free flow of information. Therefore, any anti-tracking mechanism must not destroy the existence of behavioral advertising, but instead relate more to the idea of consumer choice.

C. Privacy & Public Perception

In his famous dissent in *Olmstead v. U.S.*, Justice Brandeis described the right to privacy as "the right to be let alone."[92] The courts have gone on to find this right to privacy in the underpinnings of the amendments to the

---

87. *Id*.
88. *Id.*
89. Granted other sources of income do exist, especially in major companies that have other sources of income besides web-based advertising. Nonetheless, no company would want to constantly have a loss in any given area.
90. Rockey, *supra* note 67. (The author admits "the data is somewhat anecdotal at this point.").
91. F.T.C., PROTECTING CONSUMER PRIVACY, *supra* note 19, at 67.
92. Olmstead v. United States, 277 U.S. 438, 478 (1928).

Constitution. The Fourth Amendment and its progeny of cases would provide the basis for any argument advocating a right to privacy on the World Wide Web. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[93]

In December 2010, the Sixth Circuit Court of Appeals decided *United States v. Warshak*.[94] This case stood for the proposition that individuals possess a reasonable expectation of privacy in their e-mails, and that the government violates an individual's rights when they compel an internet service provider to turn over the contents of an individual's e-mails.[95]

Here, the Sixth Circuit looks to a line of Supreme Court cases dealing with privacy and the Fourth Amendment to reach their decision. Cases such as *Katz v. United States* and *Smith v. Maryland* have analyzed key issues such as an individual's basic expectation of privacy.[96] Justice Harlan's weighty concurrence in *Katz* provides a twofold requirement for an individual's basic expectation of privacy: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[97]

In 1979, *Smith* expounded upon another principle stated in *Katz* that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection"[98] by stating "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[99]

By applying the Fourth Amendment to e-mails, the Sixth Circuit has opened the door for other internet activity. The justification for the holding in *Warshak* rested on applying *Katz* and its progeny to e-mails and reaching the finding that society recognizes e-mails as private communication.[100] Briefly, *Warshak* found that e-mail communications have gained in societal

---

93. U.S. CONST. amend. IV.
94. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
95. *Id.* at 288.
96. Katz v. United States, 389 U.S. 347, 351 (1967); Smith v. Maryland, 442 U.S. 735, 740 (1979).
97. *Katz*, 389 U.S. at 361.
98. *Id*. at 351.
99. *Smith*, 442 U.S. at 740.
100. *Warshak*, 631 F.3d at 284-86.

importance, and if the Court in *Katz* found a privacy right in a telephone call, then surely they would find one today in an e-mail communication.[101]

In its opinion, the court also referenced *Kyllo v. United States*, which stood for the proposition that advances in technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment."[102]

The line of Supreme Court cases interpreting the Fourth Amendment, including *Warshak*, beg the question of whether 'Do Not Track' would not only expand the right to be let alone, but also start implicating Fourth Amendment issues. The article *Will the FTC's 'Do Not Track' Proposal Spell the End of Free Internet Content* states that:

> [W]hile there does appear to be a qualitative difference between physically venturing beyond your front door and venturing onto the internet, analogizing Do Not Track to Do Not Call and Do Not Mail obscures these differences and leads the FTC to propose a substantial expansion of personal privacy beyond prior constitutional notions without fully acknowledging this expansion or its potential repercussions.[103]

The underlying factual background for this argument understands that internet users make affirmative decisions to connect to the internet and request web-based content from a distant server for download and display on their internet capable device.[104] The argument follows that because consumers request access to websites created and hosted by others and because they make themselves "observable"[105] to the host system through the connection between a server and an internet capable device, that these actions are not private.[106]

While 'Do Not Track' does not specifically discuss Fourth Amendment implications, *Warshak* and commentators indicate that one's actions via the internet could have privacy repercussions. Before turning towards any analysis regarding the privacy implications of 'Do Not Track,' one must first examine statistical data, which would provide a foundation for any such argument.

In a collaborative report and survey by the University of Pennsylvania and the University of California, Berkeley, entitled *Americans Reject Tailored Advertising: and Three Activities that Enable It*, research found

---

101. *Id.*
102. Kyllo v. United States, 533 U.S. 27, 34 (2001). This case dealt with the use of thermo imaging technology to view into a house to see if heat lamps were being used to grow marijuana. The Supreme Court found this to be a search in violation of the Fourth Amendment.
103. Rockey, *supra* note 67.
104. *Id.*
105. This refers to a server recognizing an internet-capable device's IP address.
106. Rockey, *supra* note 67.

that a majority of adult Americans (66%) "do not want marketers to tailor advertisements to their interest."[107] Going further, "when Americans are informed of three common ways marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%—say they would not want such advertising."[108] The opinions did not change that much even when told that tracking occurs anonymously with 68% stating they would not allow such a practice and 19% saying they would probably not allow such a practice. Even the younger generations met online behavioral advertising with disdain. For example "55% of 18-24 year-olds do not want tailored advertising" and "86% of young adults do not want tailored advertising if it is the result of following their behavior on websites other than one they are visiting."[109] This report and survey revealed a plethora of other important statistics; for example, "[a] majority of Americans . . . do[] not want discounts or news fashioned specifically for them, though the percentages are smaller than the proportion rejecting the ads," and "69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them."[110] Turning towards both individual expectations and societal expectations, "92% agree there should be a law that requires 'websites and advertising companies to delete all stored information about an individual, if requested to do so,'" and "63% believe advertisers should be required by law to immediately delete information about their internet activity."[111] Finally, Americans wrongly assume that government regulations prohibit selling widespread data about them, and Americans also believe in strict punishment for information offenders, which could signal the public's frustration over privacy issues.[112]

Turning towards analysis under the *Katz* test, the test states "that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[113] While the study performed by the University of Pennsylvania and the University of California, Berkeley does not directly answer the question of individual and societal expectation of internet privacy, it does draw a reasonable inference. The study clearly shows that a majority of Americans reject the idea of being tracked on the internet for the purpose of generating targeted ads. The reasonable inference here is that people do not want their actions to be followed on the internet, even

---

107. Turow, *supra* note 6, at 3.
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.* at 4.
113. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

when it relates to something as small as the type of ad which appears in a box off to the side of whatever web page they are viewing. Given that this feeling permeates throughout society, one could hypothesize that some individuals, and possibly society, have a reasonable and recognizable expectation of internet privacy. Moreover, people use computers for private information; people use the internet for private transactions. For example, internet banking has increased in use over the last decade, and people would consider their bank records private information. The many uses of the internet confound the normal lines of privacy. One would easily argue that an open blog is not a private place, and that no one should have an expectation of privacy there; on the other hand, e-mail utilizes the internet to send messages and the Sixth Circuit has found such an expectation of privacy. The fact that some people believe in a right to internet privacy, coupled with the personal nature of a computer along with "private" aspects of the internet, poses questions which should be answered. Arguments, however, exist on the other side of the spectrum. For example, one could argue that the internet merely provides a medium of travel, and the Supreme Court found that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[114] This can be easily portrayed in a hypothetical. Imagine driving to Staples to buy several boxes of paper, a task that could also be done online. Given the analogy to the internet as a medium of travel, and given the argument above regarding contacting an outside server, one can argue that individuals and society as a whole should not have a privacy expectation when it comes to some uses of the internet.

If a court finds such a privacy expectation, online behavioral advertising would go by the wayside. The arguments and statistics demonstrate that the internet is a rare breed. Nothing else like it exists, and it cannot be dealt with by an overarching proposition. Time will further identify the societal expectations of internet privacy, but the sheer size and complexity of this entity may make an all encompassing privacy expectation futile.

V. PROPOSAL

This comment does not seek to provide the algorithm to ensure a perfect balance between privacy, security, and marketing. Rather, it seeks to explore the current field of online behavioral advertising and privacy implications, and bring forth a policy-based argument to the table. Arguments propounding the end of free-based web content harbor a narrow

114. United States v. Knotts, 460 U.S. 276, 281 (1983).

and extreme view of the picture. Arguments advocating the widespread misuse of your information represent the extreme at the other end of the spectrum.

The three main browsers—Internet Explorer, Mozilla, and Google Chrome—all possess privacy features which internet users may take advantage of to limit the information they convey on the World Wide Web. Internet Explorer allows a user to raise and lower restrictions on cookies. Internet Explorer also has a separate browsing function known as "InPrivate" which lets an individual surf the web without leaving an internet trail; furthermore, InPrivate accepts cookies and temporary web files needed for a browsing session, but this information is discarded upon closing the InPrivate browser.[115] Mozilla offers a setting with the same namesake as the proposed FTC regulation—'Do Not Track'—which tells websites you visit that you do not want your browsing behavior tracked.[116] Google Chrome also permits individuals to not only change their settings in regards to cookies, but also enables them to change their settings in regards to flash cookies.[117] Furthermore, Google Chrome has its own version of InPrivate referred to as incognito mode.[118]

These steps taken by the most widely used internet browsers demonstrate a strong argument against proponents advocating the elimination of online behavioral advertising. Besides the steps taken by Internet Explorer, Mozilla, and Google Chrome to protect and limit the information an individual conveys, the economic scheme of capitalism demands profits which in turn supports advertising. The question becomes when does the balance tip? When does targeting an advertisement go too far?

Three problems exist within the current framework as it pertains to online behavioral advertising. First, people lack knowledge when it comes to internet functionality and protection. While the internet becomes more user friendly practically every day, the simplicity of use undermines any desire to obtain a basic understanding. As a result, people fail to comprehend the extent of their actions online, and they maintain little understanding of the information that is actually transmitted. Second, with such a widespread lack of knowledge at the individual level, the current scheme of privacy offered by the major web browsers, albeit not difficult, needs to be made easier. Finally, 'Do Not Track' fails to adequately address the most key provision for regulation, enforcement.

---

115. *What is InPrivate Browsing*, WINDOWS, http://windows.microsoft.com/en-US/windows-vista/What-is-InPrivate-Browsing (last visited Apr. 20, 2011).
116. *How do I turn on the Do-not-track feature?*, *supra* note 80.
117. Chan, *supra* note 70.
118. *Id.*

While the three major web browsers have made great headway in offering anti-tracking technology, they have done little in the way of prominence, simplicity, and enforcement. Prominence and simplicity can be easily rectifiable by the web browsers themselves, if they so choose. The FTC's 'Do Not Track' proposal suggests a permanent cookie on a web browser. This proposal would be readily prominent, and a permanent cookie would be simple to use in comparison to the current anti-tracking means under the three major web browsers. Moreover, the FTC proposition advocates an opt-in approach, which would save a shock to online behavioral advertising. The difference between an opt-in approach and an opt-out approach is that an opt-in function would make consumers decide whether or not they wanted behavioral advertising. This would save advertising networks from losing potential, nonchalant consumers under an opt-out approach.

The main issues that must be resolved when it comes to 'Do Not Track' are enforcement and self versus governmental regulation. As noted above, companies have an inherent bias against self-regulation. Only if the countervailing forces of public perception, negative media exposure, competition, and pressure from the FTC swing the pendulum the other way would self-regulation be effective. However, effective does not mean the best decision. Without a law, enforcement of consumers' wishes regarding tracking will continue to be a problem. Companies will not follow consumer wishes, and consumers will not have any remedy against these companies. Even with a law though, the size and complexity of the internet would make enforcement a gigantic task and most likely extremely costly as well. Furthermore, proving that a company tracked an individual user would present large hurdles. These problems have no easy solution. One could propose an individual cause of action, but then proving the case would be difficult. As a result of these things, self-regulation which overcomes the problems of prominence and simplicity, and provides a robust self-enforcement framework seems to be the most effective solution under a cost benefit analysis. Only time will tell though if the countervailing forces of public perception, negative media exposure, competition, and pressure from the FTC will do a good enough job.

VI. CONCLUSION

Consumers do not like the idea of being tracked. People are private, and they do not like knowing someone is following them. The internet presents an entity unlike any other, and its functionality to society is tremendous. An inherent trade-off currently exists where network advertisers follow individuals' internet movements in order to provide targeted advertisements to that user. This has the benefit of offering greater

relevancy in ads to the consumer and greater profits for the company. However, people find this practice disconcerting.

The current anti-tracking measures that exist under the newest version of the three major web browsers seem to be a step in the right direction. If companies follow consumer wishes then no problems should arise. However, before even summing up the issue of enforcement, all three major web browsers could make headway in terms of making their anti-tracking mechanism both more prominent and simple. Regarding enforcement, it boils down to a cost-benefit analysis. The FTC would need statutory regulation in order to enforce any type of violation beyond a company's own violation of their privacy agreement. Furthermore, the sheer size and complexity of the internet would make a governmental regulatory scheme either extremely costly or ineffective. As a result of these things, governmental regulation seems too costly to be effective, but at the time of this comment, momentum seemed to be growing in Congress for such a law. In conclusion, while it may take time and while some companies may abuse the current framework, a self-regulatory scheme that focuses more on prominence, simplicity, and self-enforcement seems to be the best choice.