TAKING MATTERS INTO ITS OWN HANDS: WHY CONGRESS SHOULD PASS LEGISLATION TO ALLOW THE FTC TO REGULATE CONSUMER ONLINE PRIVACY WITH A "DO NOT TRACK" MECHANISM

Angelica Nizio[*]

TABLE OF CONTENTS

* J.D., University of Illinois College of Law, 2014. B.S., Psychology, University of Illinois at Urbana-Champaign, 2011. I would like to thank the JLTP editors for all their hard work. I would also like to thank Professor Jay Kesan, Igor Shleypak, and Rob Owen for their valuable insight. Most importantly, I would like to thank my family and friends for their infinite love and support.

I. INTRODUCTION

According to a study conducted by the Berkeley Center for Law and Technology, a majority of Americans do not want their online access information to be collected and used by advertisers.[1] Studies demonstrate that Americans perceive their Internet activity as very well protected under privacy laws.[2] Unbeknownst to most, their online behavior is being tracked extensively. Although online behavioral tracking is relatively unregulated, the Federal Trade Commission (FTC) is taking steps to keep consumers informed regarding advertisers' access to their information and to provide consumers with avenues to limit the information gathered.[3]

The FTC is a government agency that has the power to protect consumer privacy on the Internet.[4] Its mission is "to prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity."[5] Due to lack of self-regulation in the online behavioral advertising industry,[6] the FTC recommended that businesses and policymakers limit tracking of consumers' behavior on the Internet to protect consumers' privacy.[7] These recommendations included a mechanism named "Do Not Track."[8] Much of the industry has implemented the recommendations precisely; however, some

1. Chris Jay Hoofnagle et al., *Privacy and Modern Advertising: Most US Internet Users Want "Do Not Track" to Stop Collection of Data About Their Online Activities*, AMSTERDAM PRIVACY CONF. 2012, Oct. 8, 2012, at 11, *available at* http://ssrn.com/abstract=2152135 (citing a study which revealed that 60% of Americans want Do Not Track to prevent websites from collecting any information about them, 20% of Americans want it to block websites from showing them advertisements, 14% want it to prevent websites from tailoring advertisements to them based on websites they had visited in the past, and 6% of people do not know what they prefer or refused to answer).

2. *Id.* at 1.

3. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS i–vi (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC PRIVACY REPORT 2012].

4. *About the FTC*, FED. TRADE COMMISSION, http://www.ftc.gov/ftc/about.shtm (last visited Feb. 25, 2014).

5. *Id.*

6. The online behavioral advertising industry consists of tracking consumers' online activities in order to provide them with tailored advertising.

7. FTC PRIVACY REPORT 2012, *supra* note 3, at 15.

8. *Id.* at v.

members have come up with alternatives to the proposed mechanism[9] and others have executed the recommendations in a different manner due to varying external motivations.[10]

This Note will attempt to demonstrate why the industry's self-regulation is insufficient to satisfy the FTC's recommendations and why legislation is necessary as the affected parties cannot reach a consensus about what the Do Not Track mechanism should encompass. Part II of this Note will provide an overview of what online behavioral tracking is and the danger associated with it. It will also discuss the need for government intervention, why the FTC should intervene, and how the Do Not Track mechanism arose and what its goals are. Part III will explain the varied approaches organizations have taken to implement the mechanism. It will describe the pushback the FTC received from advertising organizations such as the Digital Advertising Alliance (DAA) and the recent acceptance and implementation by various companies. This Part will evaluate Microsoft's implementation of a default opt-out mechanism, which signals to advertisers by default that a user opts-out of tracking and Google's approach, which gives consumers the choice to opt-out of tracking. It will also evaluate what the online behavioral advertising industry has done since these mechanisms were implemented.

Part IV will argue that the DAA's self-regulation alternative is insufficient relative to achieving consumer privacy and that Microsoft's implementation of a default opt-out alternative does not provide consumers with adequate choice. It will argue that despite the opt-out by choice method being the optimal of the three, it will fail to achieve universal implementation if the market is left to regulate itself. This Note will demonstrate that legislation needs to be enacted, and the FTC needs to focus on mechanisms through which the consumer is aware of exactly how she is being tracked.

II. BACKGROUND

A. How Online Behavioral Tracking Works

Online behavioral tracking consists of tracking consumer online activities in order to provide tailored advertising.[11] The process is invisible to consumers but generates ads that are related to their online browsing history.[12] There are three main types of online behavioral tracking: first-party tracking, third-party tracking, and tracking through Internet Service Providers (ISPs).[13]

---

9. *See infra* Part III.A.1.

10. *See infra* Part III.

11. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2–3 (2009), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

12. *Id.* The lack of transparency is one of the main things that the FTC is concerned with and will be addressed *infra* Part II.E.3.

13. *See* Zachary Rodgers, *ISPs Collect User Data for Behavioral Ad Targeting*, CLICKZ (Jan. 3, 2008), http://www.clickz.com/clickz/news/1709905/isps-collect-user-data-behavioral-ad-targeting ("[N]umerous [ISPs are] using or testing technologies that track their subscribers' online activities and serve [advertisements]

First-party tracking involves installing a cookie[14] on the consumer's computer whenever she visits a website enabling the site to remember user preferences when the consumer accesses the same website again at a later time.[15] This type of tracking can also remember personal information that the consumer enters into the website so it can send targeted ads.[16] To tailor ads to the consumer's online activities, the advertiser places a cookie on the consumer's computer that is linked to non-personally identifiable information—"the web pages the consumer has visited, the advertisements that the consumer has been shown, and how frequently each advertisement has been shown."[17]

Third-party tracking is more invasive; it involves an ad network that contracts with advertisers and websites to deliver advertisers' ads to various websites.[18] The ad network contracts with a large amount of websites and can track an individual consumer's behavior as she browses websites in its network.[19] When websites contract with ad networks, these websites obtain access to all of the information that the network gains from other websites' contracts.[20] This is what enables the network to serve consumer ads that are tailored to the consumer's interests.[21] If a consumer happens to enter personally identifiable information into one of the websites, her name will be linked to the rest of the information that the ad network has already stored

based on those behaviors."); *AllAboutCookies.org – FAQ Section*, ALL ABOUT COOKIES, http://www.allaboutcookies.org/ad-serving/ (last visited Feb. 25, 2014) ("Third-party [tracking consists of] visit[ing] a website like allaboutcookies.org where the content . . . comes from the site, but the advertisements come from another . . . website. . . . [These cookies] allow advertisers to . . . track . . . how many people visited the advertisers' websites."); *Simple Behavioral Advertising*, CENTER FOR DEMOCRACY & TECH. (Oct. 27, 2009), http://www.cdt.org/privacy/targeting/simple.php (noting that first-party tracking uses cookies to track online behavior by keeping track of the items viewed and perhaps other information as well, such as the length of time on a webpage and the likelihood of a consumer actually making a purchase).

14. *Some Key Behavioral Advertising Terms*, CENTER FOR DEMOCRACY & TECH. (Oct. 27, 2009), http://www.cdt.org/privacy/targeting/terms.php ("A cookie is a small piece of text that a Web site saves on your computer and retrieves when you revisit that Web site. Cookies used for behavioral advertising usually contain text that uniquely identifies your Web browser, so that advertisers or ad networks can recognize the same Internet user across different Web sites or multiple times on the same site.").

15. *See Simple Behavioral Advertising*, *supra* note 13 (stating that the site stores your information on a database after it keeps track of items viewed, length of time spent on a page, and how close you were to making a purchase).

16. *Id.*

17. *Id.* It has been demonstrated that even though companies claim that an individual's identity can be kept completely separate from their cookies and browsing history, there have been instances where an individual's identity has been revealed. *Id.* Furthermore, there is always the possibility of hackers getting access to the cookies. *Id.*

18. *See Behavioral Advertising Across Multiple Sites*, CENTER FOR DEMOCRACY & TECH. (Oct. 27, 2009), https://www.cdt.org/content/behavioral-advertising-across-multiple-sites (stating that an ad network deposits a cookie on the consumer's computer and tracks the consumer throughout her entire browsing experience across multiple sites).

19. *Id.*

20. *See id.* ("This behavioral advertising model is used by dozens of ad network companies across thousands of the Web's most popular web sites."). Many consumers are completely unaware of these practices, but the practices have continued, unregulated until the FTC proposed this mechanism.

21. *Id.* ("For example, based on your visit to SF-hotel-review.com, the ad network might surmise that you're planning a trip to San Francisco. The next time you visit a Web site in the network, you might see an ad about travel to California.")

about her.[22] The ad network might also try to learn more about her by searching public databases or purchasing extra data from other companies.[23]

First-party tracking differs markedly from third-party tracking. First-party tracking is based on consumer access to a party's website.[24] All of the information that is gathered is because the consumer voluntarily accessed that website.[25] It is gathered to better meet the needs of individuals who use the website. Third-party tracking involves several entities—websites, advertisers, and networks—turning online behavioral tracking into an advertising business instead of a mechanism intended to improve consumer experience.

The newest and most complex form of behavioral advertising is even more indicative of the advertisers' self-serving interest and lack of focus on the consumer. It incorporates ISPs, which are companies that sell Internet service to consumers.[26] In ISP behavioral advertising, the ad networks contract with ISPs to collect data about their subscribers.[27] The ISP ships its subscribers' browsing activity to the ad network, which then analyzes consumer activities, creates a profile for the individual consumer, and tailors ads to their supposed preferences.[28]

This form of advertising involves even more entities than third-party tracking and has the potential to allow advertisers to gain a great deal of insight into an individual's preferences.[29] The ad networks contract with ISPs in lieu of individually contracting with multiple websites and are able to track users through one avenue.[30] This method exploits consumer information by using it without notice to the consumer in ways she would never have imagined or consented to.[31] This kind of behavioral tracking may violate federal wiretap laws, unless there is consent from the consumer.[32] ISPs such as AT&T, Verizon, Comcast, and Time-Warner each committed to refraining from such behavioral advertising without consent.[33] However, their words of commitment do not suffice, just as commitment from members of the market to follow the DAA's self-regulatory approach was not enough.[34]

---

22. *Id.*

23. *Id.* (explaining that your information has then been essentially disseminated among a variety of places).

24. *Simple Behavioral Advertising*, *supra* note 13.

25. *Id.*

26. *See Behavioral Advertising Across Multiple Sites*, *supra* note 18 (stating that companies have just begun experimenting with this type of online behavioral advertising).

27. *Id.* (discussing how ad networks sign contracts with the ISPs instead of signing contracts with a multitude of websites).

28. *Id.*

29. *Id.*

30. *Id.*

31. *Online Behavioral Advertising: Discussing the ISP-Ad Network Model*, CENTER FOR DEMOCRACY & TECH. (Sept. 18, 2008), https://www.cdt.org/policy/online-behavioral-advertising-discussing-isp-ad-network-model ("Absent unmistakable notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications.").

32. *Id.*

33. Hogan Lovells et al., *Privacy: Behavioral Marketing Gets Global Attention – ISPs in the Cross-Hairs*, LEXOLOGY (June 11, 2009), http://www.lexology.com/library/detail.aspx?g=61be473a-57cd-456a-99c5-21a31cf52eca.

34. *See infra* Part III.A.I. (discussing the DAA's self-regulatory approach).

B. The Danger of Online Behavioral Tracking and the Need for Intervention

Even if the danger of online behavioral tracking stemmed purely from harm to consumers' privacy because of ignorance regarding how information was being tracked, that would be enough to warrant intervention.[35] However, as demonstrated, the harm surpasses injury to the person. "[T]he monitoring of users' online behavior has become increasingly sophisticated."[36] It has evolved from the use of cookies to advanced third party tracking.[37] Current tracking technology even includes tools that "surreptitiously re-spawn themselves . . . after users try to delete them."[38] Although online behavioral tracking is not a new concept, it is growing so powerful that even some of America's biggest sites claim they were unaware "that they were installing intrusive files on visitors' computers."[39]

The most grave privacy concern stems from new technology, including smart phones and social media, which increases the likelihood that unidentifiable consumer information will evolve into personally identifiable information (PII)—information that "can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[40] Such activity will result in making private consumer information widely available after minimal investigation because behavioral profiles are accumulating a "myriad of personal information" at an expeditious rate.[41] The worst case scenario, according to a privacy advocate with the non-profit Consumer Watchdog, is that "[i]f the data is there, it is potentially something that could be obtained by government law enforcement authorities without you knowing about it . . . . It could potentially be subpoenaed in civil trials again."[42]

Consumers need to be aware of potential privacy intrusions and provided with avenues to protect themselves. They should be able to opt out of tracking technology, even if it only allegedly collects their non-PII, or at least be made aware of the potential disclosure of their private information.[43]

Privacy concerns can be countered by changes made within the market

---

35. Joanna Penn, *Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet*, 64 FED. COMM. L.J. 599, 608 (2012).

36. Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29, 34 (2010).

37. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404 ("[N]ation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning. A dozen sites each installed more than a hundred.").

38. *Id.*

39. *Id.*

40. *Personally Identifiable Information (PII)*, U.S. GEN. SERVICES ADMIN. (May 21, 2012), http://www.gsa.gov/portal/content/104256.

41. *See* Penn, *supra* note 35, at 606 ("Names, email addresses, and phone numbers found on social media sites can be linked with location tracked on a mobile device or data saved on retailer's sites, completing what was once an unsolvable puzzle.").

42. Sarah Kessler, *Online Behavior Tracking and Privacy: 7 Worst Case Scenarios*, MASHABLE (Nov. 3, 2010), http://mashable.com/2010/11/03/behavior-tracking-privacy/.

43. *See* Penn, *supra* note 35, at 606 (noting how quickly non-PII information can turn into PII).

and self-regulation or alternatively, by government regulation.[44] Although some argue that self-regulation will allow the market flexibility in adapting to new technologies and online behavioral tracking,[45] the market is not adapting quickly enough. Proponents of self-regulation argue that regulators should give the industry time to determine whether self-regulation methodologies are successful.[46] However, as evidenced by the rapidly advancing behavioral tracking, new technologies, and a lack of minimal protection afforded to consumers even two years after the FTC's original proposal,[47] there is a need for intervention.

C. Why the FTC Should Intervene

Congress authorized the FTC to adopt regulations for industries to follow to achieve consumer privacy.[48] Specifically, "[u]nder Section 18 of the FTC Act, 15 U.S.C. Sec. 57a, the Commission is authorized to prescribe 'rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce' within the meaning of Section 5(a)(1) of the Act."[49] Given the deceptive nature of extensive online behavioral advertising,[50] Congress should empower the FTC to regulate deceptive consumer practices through legislation that incorporates a Do Not Track mechanism. This type of legislation, which was originally proposed by consumer advocates, will allow the FTC to regulate the industry by furthering methodology that originated from within the market, instead of empowering the FTC to form its own, original regulations.[51] The result will be collaboration between the changes the members of the industry wanted to make and the government-enforced, uniform standard.

D. How the Concept of Do Not Track Arose

Consumer advocates proposed a Do Not Track mechanism in October 2007, which encompassed the idea of installing a cookie on consumers'

---

44. Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 393 (2013).

45. Catherine Schmierer, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, 17 RICH. J.L. & TECH. 13, 76 (2011).

46. *Id.* ("[T]he advertising industry has only recently taken steps to ensure that its members comply with the FTC's self-regulatory model.").

47. *See infra* Part II.E.2.

48. 15 U.S.C. § 46(g) (stating that the commission has the power to "make rules and regulations for the purpose of carrying out the provisions of this [Act]").

49. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION (July 2, 2008), http://www.ftc.gov/ogc/brfovrvw.shtm ("The statute requires that Commission rulemaking proceedings provide an opportunity for informal hearings at which interested parties are accorded limited rights of cross examination. Before commencing a rulemaking proceeding the Commission must have reason to believe that the practices to be addressed by the rulemaking are 'prevalent' (15 U.S.C. Sec. 57a(b)(3)).").

50. *See supra* Part II.A.

51. Jessica Guynn, *FTC Calls on Online Ad Industry to Agree on Do-Not-Track Standard*, L.A. TIMES (Apr. 17, 2013), http://articles.latimes.com/2013/apr/17/business/la-fi-tn-ftc-online-ad-industry-do-not-track-20130417.

browsers that would inform websites of whether the user wanted to be tracked.[52] After the proposal of this mechanism by consumers, the FTC addressed the privacy issues with regard to online behavioral advertising.[53] The FTC held a forum to discuss privacy issues with the public;[54] however, the first real development in online consumer privacy did not occur until the FTC released a privacy report in 2010.[55] The report focused on the idea that some companies do not adequately protect the information they gain from consumers, and therefore, the industry needs more policing.[56] The report recognized the growth of the online consumer culture and sought to balance consumer online privacy with helpful innovation that requires consumer data.[57] It further addressed previous unsuccessful mechanisms that were designed to protect consumer privacy.[58]

The report proposed a framework for consumers, businesses, and policy-makers regarding the collection of consumer data.[59] The framework stressed the importance of "privacy-by-design" which would be implemented by mandating: (1) privacy protections in everyday practices; (2) streamlined and simpler consumer choice for practices outside of the consumer authorized scope; (3) transparency of practices for consumers; and (4) education of consumers regarding "commercial data practices."[60] The FTC wanted to focus on "privacy, transparency, business innovation and consumer choice" because self-regulation of the industry was not sufficient.[61] Industry efforts had "been too slow, and . . . failed to provide adequate and meaningful protection."[62] The agency realized that consumers could benefit from online tracking but wanted to give consumers an easy way to control the tracking for their privacy needs.[63]

After the FTC issued its original framework, it evaluated public

52. *FTC Testifies on Do Not Track Legislation*, FED. TRADE COMMISSION (Dec. 2, 2010), http://www.ftc.gov/news-events/press-releases/2010/12/ftc-testifies-do-not-track-legislation [hereinafter *FTC Testifies*].

53. Louise Story, *Consumer Advocates Seek a 'Do-Not-Track-List,'* N.Y. TIMES (Oct. 31, 2007), http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html. Groups such as Consumer Federation of America, World Privacy Forum, and many others voiced concern about the tracking of people's online behavior. *Id.*

54. *Id.*

55. FED. TRADE COMM'N, PRELIMINARY FTC STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter FTC PRIVACY REPORT 2010].

56. *Id.* at 44.

57. *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*, FED. TRADE COMMISSION (Dec. 1, 2010), http://www.ftc.gov/opa/2010/12/privacyreport.shtm [hereinafter *FTC Framework*] (quoting FTC Chairman Jon Leibowitz, who stated that "[t]he FTC wants to help ensure that the growing, changing, thriving information marketplace is built on a framework that promotes privacy, transparency, business innovation and consumer choice").

58. FTC PRIVACY REPORT 2010, *supra* note 55, at iii ("[T]he notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand. Likewise, the harm-based model has not addressed the reputational harm and fear of being monitored that such tracking could cause.").

59. *Id.*

60. *Id.* at v–vii.

61. *FTC Framework*, *supra* note 57.

62. *Id.*

63. *Id.*

comments and technological advances and altered its framework accordingly.[64] The changes affecting Do Not Track will be discussed further in the next Part of this Note.

After the FTC issued the framework, various versions of Do Not Track were also introduced as bills.[65] Although it seemed as though companies had begun to implement the FTC's recommendations of online behavioral advertising, and thus new legislation was unnecessary, there is continued disagreement about implementation of Do Not Track.[66] Because of the ongoing trouble with implementation, legislation has been reintroduced by various members of Congress.[67]

E. Specifics of the FTC's Do Not Track Mechanism

1. The FTC's Understanding of Current Consumer Privacy Concerns

The main concern that the FTC identified regarding online behavioral tracking was the invisibility of the process—most consumers are completely uninformed of both the information that is being gathered about them and how it is being gathered.[68] Therefore, although the FTC acknowledged that online behavioral tracking benefits consumers, it also recognized that consumers need to understand what is being done with their information.[69] The agency believed that industry efforts of self-regulation were no longer sufficient, which is why the FTC took action.[70]

---

64. *FTC Issues Final Commission Report on Protecting Consumer Privacy*, FED. TRADE COMMISSION (Mar. 26, 2012), http://www.ftc.gov/opa/2012/03/privacyframework.shtm [hereinafter *FTC Issues Final Report*].

65. Among others, the Commercial Privacy Bill of Rights Act of 2011 was introduced by Senator John Kerry (D-Mass.) and co-sponsored by Senator John McCain (R-Ariz.). Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011). The Do Not Track Me Online Act was introduced by Representatives Speier, Hastings, and Filner. Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011). The Consumer Privacy Bill of Rights was introduced by President Obama. Press Release, The White House, Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

66. *See* David Goldman, *Do Not Track Is Dying*, CNN MONEY (Nov. 30, 2012, 2:56 PM), http://money.cnn.com/2012/11/30/technology/do-not-track/index.html (stating that even after months of discussion, there is no consensus on what the term "tracking" means).

67. Senator Jay Rockefeller of West Virginia reintroduced a Do Not Track Bill in March 2013 that would obligate companies to comply with Do Not Track and would give the FTC the authority to pursue enforcement action against any party that did not. Do Not Track Online Act of 2013, S. 418, 113th Cong. (2013). The bill was originally introduced in 2011 "to provide Americans with the ability to opt out of having their online activities tracked. . . . [but] would preserve the ability of online companies to conduct their business and continue to deliver content and services to customers." Press Release, Jay Rockefeller for West Virginia, Rockefeller Introduces Do-Not-Track Bill to Protect Consumers Online (Mar. 1, 2013), *available at* http://www.rockefeller.senate.gov/public/index.cfm/press-releases?ID=deb2f396-104e-46a0-b206-8c3d47e2eed3.

68. *FTC Testifies*, *supra* note 52 ("David Vladeck, Director of the FTC's Bureau of Consumer Protection . . . [said] that the practice of tracking consumers' activities online to target advertising, known as behavioral advertising, holds value for consumers because it supports content and services on the Web and delivers more personalized ads. He noted, however, that more transparency and consumer control regarding the practice are needed.").

69. *Id.*

70. *Id.*

In order to address the existing serious privacy issues and put consumers in control, the FTC proposed a Do Not Track mechanism, originally introduced by consumers, as a setting on consumers' Web browsers.[71] The idea behind Do Not Track was to install a setting similar to a cookie on each individual consumer's browser that would inform websites of whether the user wants to be tracked.[72] An initial proposal of the mechanism was made in 2010 along with other recommendations.[73] This Note will not describe the 2010 proposal in detail, but the next Part will examine the revisions that were made to the proposal and how the revisions were incorporated into the final privacy proposal issued by the FTC.

2. What the FTC's Report Proposes: How This Report Differs from the 2010 Report

In March 2012, the FTC issued its final report on protecting consumer privacy, including three revisions to the original report after public comments and technological evolutions were considered.[74] First, the revised version changes the scope of the guidance in that smaller businesses do not need to abide by the framework as long as they only collect and do not transfer non-sensitive data from fewer than 5,000 consumers a year.[75] With regard to the privacy concern, the first revision also specifies that information is not "reasonably linked" to the consumer, or computer, if "a company takes reasonable measures to de-identify the data, commits not to re-identify it, and prohibits downstream recipients from re-identifying it."[76] This revision was made in response to a multitude of comments concerning technological advances and the impact they will have on keeping consumers linked to data.[77] Second, the report improves the guidance given as to what kind of choice companies should provide consumers regarding use of their data.[78] Lastly, the report gives recommendations on how to increase transparency between data brokers and consumers.[79]

The second revision is most relevant to deciding how to best implement Do Not Track because it focuses on what kind of choice the mechanism should provide to consumers.

---

71. *Id.* (stating that online behavioral advertising "is largely invisible to consumers, and they should have a simple, easy way to control it").

72. *Id.*

73. *Id.*

74. *FTC Issues Final Report*, *supra* note 64.

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.* The report states that whether or not the consumer should have a choice in how they are being tracked depends on whether the practice is consistent with the existing relationship the consumer has with the business or if the transaction is something they clearly did not agree to. *Id.*

79. *Id.* The report supports consumers having access to data broker's information and recommends that data brokers compile their data into a website where consumers could learn more about data brokers' practices. *Id.*

3. What the Privacy Framework Addresses

As a whole, the privacy framework focuses on the same few principles that the preliminary report focused on—privacy by design, simplified consumer choice, and transparency.[80] To achieve privacy by design, the FTC encourages companies to "maintain comprehensive data management procedures throughout the life cycle of their products and services."[81] The FTC recommends simplification of consumer choices and asks companies to provide consumers with choices when their data is being used for reasons inconsistent with the context of the transaction they engaged in or the relationship the consumer has with the company.[82] To achieve transparency, the FTC recommends that companies issue privacy notices that are clear, short, and standardized.[83] The commission also recommends that companies provide their consumers with "reasonable access" to data they have about the individual consumer and put forth greater effort in educating consumers about data privacy practices.[84]

The FTC planned on assisting with implementation of these three principles through a variety of actions and mechanisms, including Do Not Track.[85] Although the industry has already begun to implement Do Not Track, the FTC continues to work with members of the industry to complete the implementation[86] and achieve the right balance for both consumers and advertising companies. As this Note will demonstrate in Part IV, the FTC will have to take on a bigger role than merely assisting companies in implementing Do Not Track. In order to make any real progress with the mechanism, it will have to be authorized by Congress to mandate rules and regulate the members of the industry.

4. What the Do Not Track Mechanism Recommends

Specifically, the FTC states that every Do Not Track mechanism should include five key principles.[87] First, it should be implemented universally among any party that would track consumers.[88] Second, it should be easy for consumers to use.[89] Third, the choices that consumers make in regard to whether they agree to being tracked should not be overridden; they should be acknowledged and adhered to.[90] Fourth, the Do Not Track system should be comprehensive in that there should not be loopholes through which consumer data can be obtained.[91] Finally, the system should opt consumers out of all

80. FTC PRIVACY REPORT 2012, *supra* note 3, at vii–viii.
81. *Id.* at vii.
82. *Id.*
83. *Id.* at viii.
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.* at 53.
88. *Id.*
89. *Id.*
90. *Id.*
91. *Id.*

types of data collection that would be inconsistent with the transaction they entered into with the company.[92] Even if a company has a first-party relationship with a consumer, it does not mean that they can track that consumer for purposes outside the scope of their website.[93] ISPs, for example, have the ability to develop highly detailed information about their consumers because they have access to all of their browsing history, but the FTC urges companies to refrain from such action without consent from the consumer or more privacy protection.[94] The use of cookies to track consumers across various websites creates the same effect that ISPs do, but the FTC is not as concerned about that as it is with the ISPs.[95] Companies have taken the FTC's five key principles and recommendations into consideration and most have implemented Do Not Track, but have done so through contrasting methods.[96] Part III will discuss the varied approaches to implementation and how they relate to the goals that the FTC has proposed.

III. ANALYSIS

A. Contrasting Approaches to Implementing the Recommendations of the FTC

1. The DAA's Self-Regulatory Approach

There has been much pushback from advertising representatives about the implementation of Do Not Track.[97] The DAA has created its own self-regulatory approach to the FTC's recommendations and expressed reluctance to require companies to honor Do Not Track.[98]

The DAA has proposed its own cookie-based opt-out in lieu of the Do Not Track header that companies have been installing into their browsers.[99] The DAA emphasizes that it limits collection, use, or transfer of data for employment, credit, healthcare treatment, and insurance purposes, but it still allows for collection or transfer of consumer online actions relative to market research.[100] The DAA cookie does not prevent behavioral advertisers from

92. *Id.* The only acceptable reasons for collecting behavioral data beyond the purposes of the transaction are to prevent click-fraud or to collect de-identified data for analytical purposes. *Id.*

93. *Id.* at 55 (stating that the specific transaction is the only avenue through which data can be tracked).

94. *Id.* at 56.

95. *See id.* (noting that ISPs have the capability of tracking virtually all of the consumer online behavior and creating a detailed profile of the individual consumer).

96. *See infra* Part III.A.

97. Jeff Blagdon, *Do Not Track: An Uncertain Future for the Web's Most Ambitious Privacy Initiative*, VERGE (Oct. 12, 2012, 12:00 PM), http://www.theverge.com/2012/10/12/3485590/do-not-track-explained (explaining the way that Microsoft IE10 has implemented do not track and the disagreement it has caused among the advertising community).

98. *See id*. (describing the alternative that the DAA offered to implement when they stated that they would not comply with the Do Not Track mechanism that the FTC proposed).

99. Rainey Reitman, *The DAA's Self-Regulatory Principles Fall Far Short of Do Not* Track, ELECTRONIC FRONTIER FOUND. (Nov. 14, 2011), https://www.eff.org/deeplinks/2011/11/daa-self-regulation-principles-fall-far-short-do-not-track.

100. DIGITAL ADVERTISING ALLIANCE, SELF-REGULATORY PRINCIPLES FOR MULTI-SITE DATA 2–5 (2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

tracking what you do online completely; rather, it focuses on the idea of not tracking browsing history in order to tailor advertisements to the consumer personally.[101] The mechanism for informing consumers about the behavioral tracking is an icon system which allows consumers to view icons that disclose information regarding the origin of the ad and how to opt out of receiving similar ads in the future.[102]

Although some believe this mechanism balances the interests of consumers and companies, it does not meet the standards set by the FTC. One of the main principles that the FTC focused on when implementing Do Not Track was opting consumers out if the transaction was one that they did not agree to.[103] By continuing to allow collection of data within the scheme of online behavioral tracking and only ceasing to display tailored ads to the consumer, consumer information is being used for reasons other than those to which she consented. This approach gives the consumer the illusion that because ads are not being targeted at her, her browsing history is not being retained.

Despite these shortcomings, the DAA emphasized the amount of consumer control that their self-regulatory approach offers.[104] However, to sincerely take consumer interests into account, the use of consumer information needs to be disclosed to allow individual consumers to make educated decisions regarding the tracking of their Internet activity. Under this regulatory approach, companies can easily collect tracking information for their own advertising benefit as long as they are not using it to target consumers, and consumers should be made aware of this possibility.

In addition to the principles that the FTC articulated for Do Not Track, the FTC's more general privacy goals incorporated a desire for transparency.[105] The DAA's lack of disclosure regarding the tracking that they engage in is not transparent and prevents consumers from shielding themselves from the type of tracking that has the most potential to injure their privacy. A mechanism that protects only against ads targeted toward the consumer and gives the illusion of complete privacy to the consumer is anything but transparent.

Even if the self-regulatory approach met the FTC's standards, the DAA would still need to demonstrate that the rest of the online behavioral advertising market was willing and able to comply with this approach, as one of the FTC's goals with Do Not Track was universal implementation.[106] The

101. DIGITAL ADVERTISING ALLIANCE, FREQUENTLY ASKED QUESTIONS: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING IMPLEMENTATION GUIDE 1 (2010), *available at* http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Frequently%20Asked%20Questions.pdf.

102. DIGITAL ADVERTISING ALLIANCE, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 5 (2009), *available at* http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

103. *See generally supra* Part II.E.4.

104. DIGITAL ADVERTISING ALLIANCE, *supra* note 102, at 3.

105. *See FTC Testifies*, *supra* note 52, at i ("These best practices include making privacy the 'default setting' for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency.").

106. *See* FTC PRIVACY REPORT 2012, *supra* note 3, at vii–viii ("[T]he DAA has developed its own icon-

DAA "obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles."[107] However, a recent study shows that while companies committed to following the self-regulatory approach, there was still frequent non-compliance with providing consumers the option to opt out of behavioral tracking[108]—reinforcing concerns about respecting consumer choices. Consumer choice within this self-regulatory approach is already limited to specifically-targeted advertising, and if companies fail to provide consumers the ability to opt out, then consumers are not being offered any protection at all.

2. Microsoft's Default "Opt-Out" Mechanism on IE10

Although organizations like the DAA propose very limited restrictions on tracking, Microsoft—a leading web browser—has installed a much more restrictive Do Not Track mechanism which is turned on by default in all of Microsoft's new Internet Explorer 10 (IE10) browsers.[109] The mechanism informs all advertisers that any user of IE10 elects not to be tracked.[110] This is the most extreme version of the Do Not Track mechanism that has been implemented, as even the recommendations of the FTC did not suggest a default opt-out recommendation for all users.

The FTC's proposal and subsequent Do Not Track mechanism are a minimum standard set forth in order to increase and protect consumer privacy.[111] Although Microsoft's default opt-out mechanism surpasses the minimum FTC requirements by enabling Do Not Track automatically, it is the company's own prerogative to do so. Companies have the ability to ensure even greater protection than the FTC recommends. However, in addition to the FTC's efforts to protect consumers, the FTC aims to "accomplish [that protection] without unduly burdening legitimate business activity."[112]

This goal begs the question of whether the FTC would be unduly burdening the advertising industry with a default opt-out mechanism, such as the one Microsoft implemented in their IE10. Many critics state that without

based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done.").

107. *Id.* at 54.

108. Saranga Komanduri et al., *AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements*, 7 I/S: J.L. & POL'Y 603, 632–34 (2012) (demonstrating that after conducting a field study of whether or not companies were complying with the approach, a significant number of companies were found to be in non-compliance).

109. Tony Rizzo, *New 'Do Not Track' Law of the Land to Kill Microsoft IE10 Golden Goose*, TECH ZONE 360 (Oct. 10, 2012), http://www.techzone360.com/topics/techzone/articles/2012/10/10/311477-new-not-track-law-the-land-kill-microsoft.htm (stating that Microsoft claimed to be doing so in order to provide the safest online behavioral tracking option for consumers).

110. *Id.* (stating that the system automatically sends Do Not Track signal to all browsers, informing them that the consumer does not want to be tracked).

111. *See generally* FTC PRIVACY REPORT 2012, *supra* note 3 (proposing standards for protecting consumer privacy).

112. *About the FTC*, *supra* note 4.

the funding of advertisers whose tracking revenue allows them to pay for free sites and offer free access to consumers, some of the most used websites would no longer be available to the public.[113] The Association of National Advertisers stated that free web services would be threatened and the Internet would eventually be destroyed because without the ability to track, advertisers would not have a reason to pay for their presence on websites.[114]

Many smaller advertisers argue that large competitors such as Google and Yahoo do not have to be as concerned with Do Not Track because they have access to a vast amount of consumer online behavior regardless.[115] A recent study by a research firm that frequently studies local online behavioral advertising showed that Do Not Track would be detrimental to small and medium-sized businesses, as targeted display advertising makes up forty-five percent of these companies' revenue.[116]

Advertisers' inability to collect revenue from online behavioral advertising could result in a lack of free web services. The potential lack of free web services would be disconcerting to many individuals. However, according to the Interactive Advertising Bureau (IAB), the impact of a default Do Not Track mechanism would actually not be as severe.[117] Only about fifteen percent of the online advertising industry's revenue came from online behavioral advertising in 2011—making a strong argument that the industry is still sustainable even after such a change.[118] This statistic is evidence that restricting online behavioral advertising might not unduly burden the industry after all. However, when critics evaluate the effects of Do Not Track on revenue, many have not considered a mechanism enabled by default and as such have underestimated the effect of automatic opting-out.[119] The concerns with a default Do Not Track mechanism do not end there.

Despite the fact that a default Do Not Track mechanism might not be as detrimental to the advertising industry as anticipated, other issues remain. If Microsoft is the only major browser developer willing to adopt such extensive measures, this will cause problems with the FTC's principle of universal implementation. Unless the FTC recommends a default Do Not Track

113. *Internet Explorer 10 & Microsoft's 'Do Not Track' Headache*, WDHI REVIEWS – WIRELESS HDTV NEWS (Oct. 14, 2012), http://whdi-reviews.com/2012/10/internet-explorer-10-microsofts-do-not-track-headache.

114. *Id.*

115. Goldman, *supra* note 66 (explaining that major browsers share competing interests with smaller companies who cannot depend purely on the content gathered from their own network like the major browsers can).

116. BORRELL ASSOCS., MAIN STREET GOES SOCIAL: SMBS GIVE A BIG THUMBS-UP TO SOCIAL MEDIA 15 (2012).

117. Sarah Downey, *The Free Internet Will Be Just Fine with Do Not Track. Here's Why.*, TECH CRUNCH (Sept. 23, 2012), http://techcrunch.com/2012/09/23/the-free-internet-will-be-just-fine-with-do-not-track-heres-why (demonstrating that about forty-five percent of the online advertising industry's revenue came from searches, and other avenues such as classifieds, digital video, non-behavioral displays, lead generation, mobile, rich media, sponsorship, and email made up another forty percent of revenue).

118. *Id.*

119. *See id.* (stating that Do Not Track will not have as much of a devastating effect as advertisers have stated because many people will choose not to opt out, and others will not know that they have a choice to do so).

mechanism, which it likely will not because of the lack of consumer choice as discussed below,[120] other browser developers will likely abstain from adopting a mechanism that limits their ability to track consumer information and contract with ad networks. As discussed in Part II.A, third-party tracking can be a lucrative enterprise for browsers.[121] Advertisers are customers of the browsers, as advertisers contract with them for access to all of the information that the browser gains from other websites. Consumer browsing history is valuable to advertisers, and the business of advertisers is valuable to major browsers. Browser developers would be forfeiting profit from advertisers who were interested in contracting with them if they were to enable a default opt-out mechanism. When the enabling of Do Not Track is the consumer's choice, there remains a large possibility that consumers will choose not to enable the mechanism and that browsers will continue to track consumer behavior without consumer permission.[122] Therefore, major browsers are unlikely to adopt a default mechanism if the FTC recommendations do not suggest that option.

In addition to creating a problem with universal implementation, a default opt-out mechanism will not be mindful of consumer choice. Simplified consumer choice was one of the main goals of the FTC's privacy framework and was echoed in the principles concerning Do Not Track.[123] Recently, one of the FTC's own Commissioners, J. Thomas Rosch, criticized Microsoft's default opt-out mechanism for not giving consumers any say in what signal their browser will send and therefore not giving them an opportunity to control the tracking of their information.[124] Instead of educating consumers and allowing them to participate in deciding how their information is being processed, this mechanism puts all of the power back in the hands of the companies.

Although this mechanism will work to protect consumer privacy and is not unduly burdensome on the industry—at least not from a current statistical standpoint[125]—it is not the optimal way to control online behavioral advertising because it leaves the consumer uninformed and without the opportunity to choose her preferences. Furthermore, it will not achieve universal implementation because of likely reluctance from other members of the industry to comply.

---

120. *See infra* Part III.A.3 (discussing the importance of consumer choice regarding the Do Not Track mechanism).

121. *See supra* Part II.A (discussing how third-party tracking can be used to collect consumer information which can then be sold to advertisers).

122. *See infra* Part III.A.3 (discussing the likelihood that consumers will not enable Do Not Track mechanisms, thereby allowing companies to track their behavior).

123. *See supra* Part III.A.1 (mentioning consumer choice as the main principle underlying the FTC's privacy framework).

124. *See* Katy Bachman, *FTC Commissioner Blasts Microsoft Do Not Track Browser: Says Default Setting Does Not Give Consumers Choice*, ADWEEK (June 21, 2012, 10:41 AM), http://www.adweek.com/news/technology/ftc-commissioner-blasts-microsoft-do-not-track-browser-141276 ("Microsoft's default DNT setting means that Microsoft, not consumers, will be exercising choice as to what signal the browser will send . . . .").

125. *See generally id.* (discussing how the privacy mechanism is not overly taxing on consumers or browsers).

3. Google's "Opt-Out by Choice" Mechanism

Google was one of the last companies to agree to install Do Not Track on its browser.[126] The DAA finally compromised with the government and agreed to a Do Not Track mechanism, which included an opt-out setting, prompting Google to finally agree to Do Not Track as well.[127] Google decided to implement an opt-out version, which allows consumers to enable the Do Not Track mechanism, rather than installing a default opt-out setting on the browser.[128] "Google and most advertisers can live with this option. The odds remain in their favor that users simply won't turn it on and ultimately a very high percentage of tracking cookies will continue to do what they've always done."[129]

This alternative mechanism does not raise many of the same issues that the DAA's self-regulatory approach and the default opt-out mechanisms do. Given the circumstances of consumer privacy and the FTC's recommendation, of the three proposed mechanisms, an opt-out by choice mechanism seems to strike the best balance between consumers who need protection and the advertising industry which should not be unduly burdened.

Providing consumers with the choice to opt out of tracking meets the minimum standards set by the FTC.[130] If statistics show that Microsoft's default mechanism does not appear to be unduly burdensome, then a less restrictive mechanism such as this opt-out by choice mechanism cannot be either. Again, advertisers have an advantage with this mechanism, as it is likely that not all consumers will enable it.

Consumer choice to enable the mechanism provides for consumer control that the DAA's self-regulatory mechanism and Microsoft's default opt-out mechanism do not. Consumer control was part of the FTC's broader privacy framework and Do Not Track principles;[131] it is important that the consumer alone makes the decision to enable the Do Not Track mechanism. The opt-out by choice mechanism is optimal because, while many individuals are concerned with privacy, some appreciate the way that online behavioral tracking customizes their online experience for them and are willing to take the privacy risks. The consumer can decide for herself whether or not opting out is the right choice.

Despite the balance between consumers and the advertising industry, universal implementation continues to be a problem. As long as Microsoft implements a default opt-out mechanism, all major browsers will not offer customers the same Do Not Track standards.[132] As will be discussed in the

126. *See* Rizzo, *supra* note 109 (stating that Google finally agreed because the rule stated that Do Not Track would not be automatically enabled).

127. *Id.*

128. *Id.*

129. *Id.* There is a good possibility that many consumers will not enable the mechanism, however, because they are given the choice; the FTC would consider their decision to be an informed one and therefore would not be concerned with those individuals' lack of privacy.

130. FTC PRIVACY REPORT 2012, *supra* note 3, at 52–55.

131. *Id.* at 10.

132. *See* Rizzo, *supra* note 109 (discussing Microsoft's choice to implement a default opt-out option as

next Part, many members of the industry state that they will not adhere to Microsoft's demands to opt all consumers out of tracking.[133] With browsers continuing to disagree on the mechanism to adopt and refusing to recognize one another's different mechanisms, consumer privacy will continue to diminish, and consumers will remain unprotected.

B. What the Industry Has Done Since Implementation of These Mechanisms

After much debate, all major browsers except for Microsoft[134] have agreed to the opt-out by choice mechanism. As mentioned above, advertisers, marketers, and vendors say they will not enforce Microsoft's opt-out by default rule.[135]

Yahoo claims that Microsoft does not allow users any discretion in the decision and therefore does not recognize it.[136] Yahoo stressed the importance of user intent and addressed the fact that individuals might not opt out as often if the Do Not Track option is not automatically turned on.[137] While it may seem as though Yahoo is self-interested, as it might seem with many other companies, it is not in Yahoo's favor to restrict its ability to engage in online behavioral tracking even more than the FTC prescribes.

The White House demonstrated that, as major companies begin to implement Do Not Track, it would work with the Worldwide Web Consortium (W3C) to finalize the requirements of the Do Not Track mechanism.[138] The W3C "is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards."[139] The W3C has formed an opinion and ruling on Microsoft's default opt-out mechanism; its Internet standards-setting body has "preliminarily ruled that browser makers cannot set the [Do Not Track] signal for users, essentially letting each website decide whether it will acknowledge or ignore IE10's."[140] Again, this raises an issue with the universal implementation that the FTC was striving for. If it is up to the companies to decide whether to comply, and if not all companies choose to apply Microsoft's mechanism, what standard will they have to comply with in the alternative? It will be a large disservice to consumers if these companies are not restricted in their tracking of online behavior;

---

opposed to Google choosing an opt-in option).

133. *See infra* Part III.B.

134. *See* Rizzo, *supra* note 109. Microsoft had already introduced their default opt-out browser and will likely not retract it.

135. *Id.*

136. Gregg Keizer, *Yahoo to Ignore Microsoft's 'Do Not Track' Signal from IE10*, COMPUTERWORLD (Oct. 29, 2012, 3:51 PM), http://www.computerworld.com/s/article/9233030/Yahoo_to_ignore_Microsoft_s_Do_Not_Track_signal_from_IE10.

137. *Id.* This is a large advantage that a default opt-out mechanism would not offer them.

138. *See* Press Release, White House, Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b ("In response to calls from the Administration and the [FTC], leading Internet companies and online advertising networks are committing to use Do Not Track technology from the [W3C] in most major web browsers to make it easier for users to control online tracking.").

139. W3C, http://www.w3.org/Consortium (last visited Nov. 26, 2012).

140. Keizer, *supra* note 136.

Microsoft's highly restrictive measure could do more harm than good.

Recently, the DAA has left the W3C group that was finalizing the requirements of Do Not Track.[141] This demonstrates that the members of the industry are not able to come up with a method of implementation that will meet the goals of the FTC. The advertising groups and the privacy activists are at an impasse. Instead of moving closer to universal implementation, the industry is moving away from it.[142] This reinforces the need for legislation.

IV. RECOMMENDATION

The privacy report issued in March 2012 focused on five main principles regarding Do Not Track—universal implementation, ease of use, persistent recognition of consumer choice, comprehensiveness, and protecting consumers from practices inconsistent with transactions they entered into.[143] The overarching privacy principles that it hoped to achieve were privacy by design, simplified consumer choice, and transparency.[144] Part III of this Note demonstrates three main ways that key players in the industry have implemented Do Not Track. The three methods all take into account the FTC's principles and address consumer privacy. However, none of the methods on their own accomplish all that the FTC was striving for in its recommendations.

A. Legislation: The Only Solution to Achieving the FTC's Five Principles Regarding Do Not Track

1. Effect of Legislation on Universal Implementation and Comprehensiveness

Until all major players in the industry agree on a standard, universal implementation will not be possible. Companies need to agree on how to put consumers in control of tracking. Microsoft's choice to implement a default opt-out mechanism is not aiding the FTC's quest for universal implementation. If companies, such as Microsoft, choose a default setting, but other companies provide consumers a choice, then the system will not be uniform, and consumers will be offered different types of protection or will be left unprotected.

141. Kate Tummarello, '*Do Not Track' Effort in Trouble*, HILL (Sept. 17, 2013, 3:30 PM), http://thehill.com/blogs/hillicon-valley/technology/322701-do-not-track-group-should-give-up-departing-online-ad-reps-say.

142. *See, e.g.*, Keizer, *supra* note 136 (discussing Microsoft's unique stance on Do Not Track); Tummarello, *supra* note 141 ("[T]he Working Group does not have a path to consensus that includes large blocs of stakeholders with views as divergent as the DAA, on the one hand, and those seeking stricter privacy rules, on the other. I no longer see any workable path to a standard that will gain active support from both wings of the Working Group.").

143. FTC PRIVACY REPORT 2012, *supra* note 3.

144. *See supra* Part II.E.3 (explaining the three principles and what steps the FTC recommends to achieve them).

The DAA's self-regulatory approach would not aid universal implementation either because the mechanism available to consumers would not only differ from the header in Do Not Track, but also the type of information the DAA would continue to gather even with the mechanism would vary from what the other mechanisms propose. The difference in standards—mainly Microsoft's extensive mechanism—has led the W3C to preliminarily rule that default opt-out mechanisms do not have to be adhered to by websites.[145] Consumer privacy will be jeopardized if the majority of companies are instructed not to comply with an identical standard.

The principle of universal implementation impacts another principle that the FTC acknowledges the importance of—comprehensiveness of the system.[146] If companies choose not to recognize Microsoft's implementation, then they create loopholes in the system because, although Microsoft's mechanism purports to maximize protection, consumers will be exposed to the dangers of the online behavioral advertising world if every company does not acknowledge the mechanism. The principle of comprehensiveness further influences the principle of protecting consumers from tracking practices with which they do not agree. Again, without an agreed-upon standard, consumers will lack any sort of protection.

The disagreement in implementation has been ongoing since consumer advocates voiced concern about privacy and proposed a Do Not Track mechanism in 2007.[147] The FTC introduced its first proposal in 2010, which fueled the disagreement. Now, over four years later, the major players in the industry continue to disagree over how to implement a mechanism and how restrictive it should be. The FTC did stress its intent for the industry rather than the government to implement change.

The FTC was hoping that the major figures in the industry would "work collaboratively to give consumers choices about how and when they are tracked online."[148] It is apparent that working collaboratively has not yielded the results that were expected. This is especially true after an important contributor to the W3C group–the DAA–has withdrawn.[149]

The competing interests of consumers and advertisers do not allow for a

145. *See supra* Part III.B (discussing the W3C's decision to let individual websites choose whether to adhere to a default mechanism). This occurred because the W3C finds the standard too restrictive. Wendy Davis, *Web Standards Group Criticizes Microsoft's Do-Not-Track Move*, DAILY ONLINE EXAMINER (Jun. 6, 2012), http://www.mediapost.com/publications/article/176314/web-standards-group-criticizes-microsofts-do-not-.html.

146. FTC PRIVACY REPORT 2012, *supra* note 3; *see also FTC Framework*, *supra* note 57 ("The [FTC] report also recommends other measures to improve the transparency of information practices, including consideration of standardized notices that allow the public to compare information practices of competing companies.").

147. *See supra* Part II.D (discussing the 2007 proposal).

148. Jon Leibowitz, Chairman, Fed. Trade Comm'n, Prepared Remarks at Ad:Tech NY (Nov. 8, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/intersection-online-advertising-and-privacy-ftc-enforcement-policy-and-encouragement-self-regulation/111108adtech.pdf (implying that they would be able to agree on standards and the government would be able to avoid intervention by introducing and passing relevant legislation).

149. Tummarello, *supra* note 141.

middle ground that satisfies both parties.[150] Websites and advertisers need to be compelled to adhere to Do Not Track. Passing legislation would force all major browsers to adopt a universal mechanism, especially if a penalty for not adhering to the mechanism is included. This is the best solution to the ongoing debate regarding implementation of Do Not Track, which has been going on for over two years.

Although the FTC wanted to steer clear of government enforcement of a Do Not Track mechanism,[151] any legislation proposed this late in the game would inevitably be a compilation of all the existing industry efforts. Furthermore, it would adhere to the issues the FTC cautioned Congress about when legislation was considered probable.[152] Although the government would be enforcing it, the legislation would be a reflection of industry methods that best encompass the principles established by the FTC.

The view that legislation might in fact be necessary is even more evident from the recent reintroduction of a Do Not Track bill by Senator John D. Rockefeller.[153] His bill would require the FTC to prescribe regulations and would give the Commission the power of enforcement[154] along with the ability to issue civil penalties to non-compliant organizations.[155] Universal and comprehensive implementation would be achieved with the passing of legislation that includes both of those principles because the FTC would have the authority to hold industry members accountable.

2. Using Legislation to Form a Mechanism that Focuses on Persistent Recognition of Consumer Choice and Protection from Inconsistent Practices

Legislation would allow the FTC to mandate a standard for Do Not Track, which would optimize consumer privacy, allow for consumer choice, and protect consumers from transactions inconsistent with those they entered into.

---

150. *See id.* (describing the divergent views of larger companies in groups such as the DAA who are opposed to stricter privacy standards desired by consumers).

151. *See* Leibowitz, *supra* note 148 (stating that is not the FTC's place to involve itself in the economic interplay between advertisers and consumers on the Internet).

152. *See FTC Testifies*, *supra* note 52 ("If Congress chooses to enact legislation, the Commission urges Congress to consider several issues including . . . not undermin[ing] the benefits online behavioral advertising provides consumers . . . not requir[ing] a registry of unique identifiers; rather . . . a browser-based mechanism . . . consider[ing] an option that lets consumers choose to opt out completely or to choose certain types of advertising they wish to receive or data they are willing to have collected about them . . . [a] mechanism [that is] simple, and easy to find and use . . . and giv[ing the FTC] Administrative Procedures Act rulemaking and the ability to fine violators to 'provide a strong incentive for companies to comply with any legal requirements, helping to deter future violations.'").

153. Do-Not-Track Online Act of 2013, S. 418, 113th Cong. (2013).

154. *See id.* § 2 ("Not later than 1 year after the date of the enactment of this Act, the Federal Trade Commission shall promulgate regulations that establish standards for the implementation of a mechanism by which an individual can simply and easily indicated whether the individual prefers to have personal information collected by providers of online services . . . .").

155. *See id.* § 3 ("[F]or purposes of imposing a civil penalty . . . with respect to a person that violates a rule . . . the amount determined under this paragraph is the amount calculated by multiplying the number of days that the person is not in compliance with the rule by an amount not greater than $16,000.").

All three of the proposed mechanisms that were discussed in Part III of this note have positive characteristics; however, the mechanism that provides a choice to opt out is most favorable to the consumer.[156] Giving the FTC power to promulgate regulations will allow it to mandate the opt-out by choice mechanism throughout the entire industry. The DAA's approach does not optimize consumer choice because, while it provides the opportunity to use icons to opt out of personalized advertisements, it does not allow consumers to opt out of all behavioral tracking, especially the kind that goes undetected.[157] Microsoft's default opt-out mechanism does not allow consumers to make any choices at all.[158] An automatic setting such as this diminishes the amount of control that consumers can actually exert. An opt-out by choice method such as the one Google[159] and many other major browsers have adopted provides consumers with the most control over how advertisers track them. This demonstrates that the FTC is focused on protecting consumers while not impeding the industry. Authority given to the FTC by Congress will allow for enforcement of an opt-out by choice mechanism that accomplishes this.

The opt-out by choice method of Do Not Track as well as the opt-out by default method both send out headers to websites, informing them that the consumer does not want to be tracked.[160] Although a mere header does not seem optimal when companies can decide how and when to acknowledge it,[161] legislation will give the FTC authority to control both of those aspects of the mechanism.

Microsoft acknowledged, "there is no single definition of what it means to be 'tracked,' so expressing a preference does not guarantee" that websites will not track consumer information.[162] Lack of a concrete definition increases the chances that consumers are being tracked in ways that they did not agree to. In order to assure that consumer protection is consistent with what they envisioned, the FTC should define "tracking" relative to Do Not Track. The FTC should consider the current types of tracking that are being blocked by the mechanisms and formulate a standard that offers consumer protection consistent with what consumers understand the protection to be. The current Do Not Track mechanisms do not define "tracking;" websites are free to choose how they define it,[163] and as a result they are also free to choose what kind of information they gather about the consumer. The DAA's self-

156. *See* Erin Shea, *63pc of Affluent Consumers Want to Opt Out of Online Tracking*, LUXURY DAILY (March 13, 2013), http://www.luxurydaily.com/63pc-of-affluent-consumers-want-to-opt-out-of-online-tracking-luxury-institute (noting that thirty-seven percent of users would choose to be tracked).

157. *See supra* Part III.A.1.

158. *See* Rizzo, *supra* note 109 (pointing out that users must first turn on the Do Not Track mechanism and then choose to not be tracked).

159. *Id.*

160. Emil Protalinski, *Everything You Need to Know About Do Not Track*, NEXT WEB (Nov. 25, 2012, 10:00 AM), http://thenextweb.com/apps/2012/11/25/everything-you-need-to-know-about-do-not-track-currently-featuring-microsoft-vs-google-and-mozilla/#!w43jN.

161. *See Do Not Track Test Page*, IE MICROSOFT.COM, http://ie.microsoft.com/testdrive/browser/donottrack/default.html (last visited Feb. 24, 2014) (acknowledging that the Do Not Track header will not guarantee that consumer behavior will not be tracked at all).

162. *Id.*

163. Goldman, *supra* note 66.

regulatory standard for blocking tracking does not wholly shield consumers from what advertising companies are able to do with their online behavioral information.[164] The DAA gives the consumer the option to opt out of tailored ads that are presented to them but continues to collect other behavioral information that the consumer is unaware of.[165] This is equivalent to the DAA defining tracking as first-party tracking and allowing all other types. The undisclosed tracking is precisely the kind of tracking that the FTC aims to avoid as is evident from the privacy framework.[166]

The FTC, through the power that legislation would provide it, should adopt a Do Not Track standard that gives consumers the option to block any of the three existing types of tracking. Major web browsers should provide the consumer with an explanation of the different types of tracking, similar to the explanation given in Part II.A of this Note, and consumers should get to choose what tracking they find intrusive and block websites accordingly. After a brief explanation of how different types of tracking work, consumers would likely be most wary of ISP behavioral advertising, as consumer information that is collected with that method is the most comprehensive of the three.[167] Third-party tracking might also make consumers uneasy; however, many consumers might be comfortable with the idea of first-party tracking, as it enables websites that the consumer herself visited to gather data and advertise to the consumer accordingly.

Consumer choice and protection from inconsistent measures will be optimized if the FTC has the authority to formulate measures that clearly define "tracking," to provide consumers with insightful explanations followed by opportunities to restrict their tracking accordingly, and to enforce those measures accordingly.

3. Effect of Legislation on Ease of Use

The current mechanisms for curbing online behavioral tracking are relatively easy to use. The DAA's icon mechanism is self-explanatory, Microsoft's default mechanism is already enabled within the browser, and the opt-out by choice mechanism only requires changing the settings on a user's browser and within a few seconds a Do Not Track header is set up to send with his or her "browsing traffic."[168] While the mechanisms are easy to use, they are not comprehensive.[169] Therefore, while a new mechanism effectuated by legislation will not be improving upon this principle, the recommended changes set forth above will continue to keep the process simple while increasing consumer privacy and protection.

---

164. *See supra* Part III.A.1.

165. *Id.*

166. *See generally* FTC PRIVACY REPORT 2012, *supra* note 3 (discussing how the FTC is calling on companies to implement better practices to protect their consumers' data).

167. *See supra* Part II.A.

168. Alex Chitu, *Do Not Track in Google Chrome*, GOOGLE OPERATING SYSTEM BLOG (Nov. 8, 2012, 5:55 AM), http://googlesystem.blogspot.com/2012/11/do-not-track-in-google-chrome.html (explaining how to access the setting through which Do Not Track may be enabled).

169. FTC PRIVACY REPORT 2012, *supra* note 3, at 53.

V. CONCLUSION

The online behavioral advertising industry was not self-regulating at a satisfactory speed, therefore consumer advocates formulated a mechanism that would aid in providing consumers with protection and privacy.[170] The FTC took formal steps to advance that initiative. The FTC's preliminary privacy report and the final privacy report both focus on transparency, keeping consumers informed, and providing consumers with choices. Major players in the industry have recently accepted and implemented variations of Do Not Track, but none of them have done so in a way that optimally meets the recommendations of the FTC.

The variations of the Do Not Track mechanism include mechanisms that consumers have to enable themselves, self-regulatory versions that include icons rather than a Do Not Track header, and mechanisms that are enabled by default.[171] Two years after the FTC issued its first report on consumer privacy regarding the mechanism, disagreement amongst advertisers, major web browsers, and consumers about how the mechanism should be implemented still exists.[172] No comprehensive, universal mechanism has been implemented. The FTC should be given authority by the legislature to form a clear standard that members of the industry will have to adhere to. The standard should be an improved-upon reflection of what the industry has implemented up until this point. The standard should give consumers the option to opt out of any or all three types of online behavioral tracking after giving them the opportunity to learn more about what the tracking entails. Until legislation is enacted and Congress gives FTC enforcement authority, Do Not Track will not advance.

170. Story, *supra* note 53 ("A coalition of privacy groups asked the government . . . to set up a mandatory do-not-track list for the Internet."); *see also* Greg Sterling, *White House Launches "Consumer Bill of Rights" Effort, Companies Commit to "Do Not Track" Buttons*, MARKETING LAND (Feb. 23, 2012, 10:30 AM), http://marketingland.com/obama-admin-to-introduce-consumer-privacy-bill-of-rights-do-not-track-today-6637 (outlining the key principles of the Consumer Privacy Bill of Rights).

171. *See supra* Part III.A.

172. Goldman, *supra* note 66.