The Swanson Paradox: Do-Not-Track and the Intersection of Data Autonomy and the Free Market

Kyle Ferden*

* J.D., The University of Iowa College of Law, 2016; B.A., The University of Northern Iowa, 2010. I would like to thank my family and friends for their unwavering support during this amazing academic adventure. I would also like to thank Nortbert Kaut for first inspiring me to research this topic.

I. INTRODUCTION

Americans generally place high value on their personal privacy.[1] Recent studies show that Americans are hesitant to even elevate personal and national safety above their privacy concerns.[2] It may be surprising, then, that online privacy tends not to be an area of concern for many.[3] One possible reason for this lack of unease is because it is difficult to know what actually happens to our data should we choose *not* to take measures to secure it.[4] Though there is some confusion about the exact journey our data takes once it is accessible to other parties, we are subtly bombarded with evidence—should we choose to acknowledge it—that remind us we are not truly alone when we surf the Internet. It does not matter if you off-handedly searched for a pair of running shoes or if you Googled for an explanation for society's obsession with pumpkin spice, the ads in your Facebook sidebar can remind you of those browsing sessions for weeks on end.

If you have ever looked at those ads and felt mildly uncomfortable, you are among great company. Unfortunately, there are few options that make controlling your data easy, transparent, and understandable.[5] Further, the options that *are* available are not comprehensive and are filled with their own drawbacks.[6]

In the advertising industry, behavioral, targeted ads are the cheapest, most discrete, and most efficient means of tracking our (the consumer's) every click, search, and online purchase. In the age of exceedingly lengthy, and oft-ignored, privacy policies, the license to collect our very own data is handed over by little more than our own reckless fingertips. As the adage goes, "when something is free, you are the product";[7] never has this been truer than when it comes to your data.

In Part II of this note, I will outline the Do-Not-Track (DNT) mechanism—a distillation of consumer protection groups' proposals for a mechanism that gives voice to consumer tracking preferences. In addition, I will discuss the current domestic and foreign responses to the rise of behavioral tracking and how those responses have fared in recent years. Part III will analyze three of the most widely-proposed approaches for managing tracking standards in the age of behavioral marketing. Part IV will propose a practical solution based on the realities of the legislative and industry atmospheres and implementation recommendations already in place.

---

1. Associated Press, *Poll: Americans Value Privacy Over Security*, POLITICO (Jan. 27, 2014, 12:21 PM EST), http://www.politico.com/story/2014/01/poll-americans-privacy-security-102663.html.

2. *Id.*

3. *See* Josh Harkinson, *6 Reasons We Share Too Much Online, According to Behavioral Scientists*, MOTHER JONES (Oct. 1, 2013, 6:00 AM EDT), http://www.motherjones.com/media/2013/10/science-behind-why-nobody-cares-about-online-privacy ("According to a recent Pew survey, only small fractions of internet users have taken steps to avoid being observed by hackers (33%), advertisers (28%), friends (19%), employers (11%), or the government (5%)."); *see generally* Bob Al-Greene, *13 Million Facebook Users Haven't Touched Their Privacy Settings*, MASHABLE, http://mashable.com/2013/04/30/facebook-graph-search-privacy-infographic (last visited Oct. 29, 2015) (stating that most Facebook users are not aware of how to properly use privacy settings).

4. *See* Harkinson, *supra* note 3 ("Not even the experts have a full understanding of how personal data is used in an increasingly complicated market . . . .") (quoting Alessandro Acquisti).

5. Nizio, *infra* note 20 and accompanying text.

6. *Id.*

7. Scott Goodson, *If You're Not Paying For It, You Become The Product*, FORBES (Mar. 5, 2012, 12:34 PM), http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/.

II. BACKGROUND

Section II.A discusses DNT, its purpose, details regarding its implementation, and how it fits within the overall framework of the Federal Trade Commission (FTC). Section II.B expands on the flurry of proposed legislation across the United States in response to the FTC's push for broader privacy legislation. Section II.C discusses successful EU legislation and it's Data Protection Directive.

A. FTC's Do-Not-Track Framework

Consumer advocacy groups first proposed the idea of DNT—loosely based on the Federal Do-Not-Call system[8]—to the FTC in 2007.[9] These groups wanted protection from the industry practice of secretly collecting, analyzing, and sharing consumer data for advertising purposes.[10] In December 2010, the FTC issued a preliminary staff report proposing a framework to regulate the ways advertisers utilize consumer information with regard to a consumer's browsing and search activities.[11] The report acknowledged that online privacy was much more complex than simply "a right to be let alone."[12] The proposed framework was a direct response to the data concerns outlined above and built upon the notice-and-choice model that the FTC had previously adopted.[13]

The framework called for three elements to be present in any future online privacy regulations. First, privacy by design, a system by which companies promote privacy protections throughout their organizations and during development, implementation, and servicing.[14] Second, simplified choice means that companies can use their discretion in denying customers with choices in "commonly accepted" practices, however, they must provide customers the chance to make conscious decisions about their data and abide by a

8. *See Hearing on A Status Update on the Development of Voluntary Do-Not-Track Standards Before S. Comm. on Commerce, Sci, & Transp.*, 113th Cong. 4 (2013) (statement of Justin Brookman, Director, Consumer Privacy, Center for Democracy and Technology), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf (proposing that advertising entities provide their domain name and server information to the FTC so that the Commission could maintain a database for consumers to download, browse, and sign up for a comprehensive, or selective, DNT List).

9. Joshua A.T. Fairfield, *Do-Not-Track as Default*, 11 NW. J. TECH. & INTELL. PROP. 575, 581 (2013).

10. Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 283 (2012).

11. *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*, FED. TRADE COMM'N (Dec. 1, 2010), http://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers.

12. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

13. *See id.* (noting that the FTC recognized that the notice-and-choice model—the policy they had implemented with the purpose of increased transparency by online businesses—led to "long, incomprehensible privacy policies that consumers . . . do not read, let alone understand").

14. *See id.* at 40 (suggesting that by shifting the requirement on companies to integrate privacy protections into their "regular business operations and . . . product development," it reduces the burden on consumers to "seek out . . . privacy protective data practices" themselves); *see also id.*at 13–15 (stating specifically that potential means of protection employed by a company should include various approaches to data minimization, retention limitation, and data quality).

DNT mechanism once the user has made his preferences known.[15] Third, the framework requires increased transparency so that users can easily understand the information in a given business' stated privacy policies.[16]

The public response following the preliminary report centered mainly on the FTC's recommendation of a DNT mechanism that would communicate consumer privacy preferences.[17] Essentially, the proposed DNT mechanism consisted of a piece of code written into a user's web browser that would send a signal expressing the user's tracking preference (either allowing or barring data tracking by a particular website).[18] Further, the expression would send a request (depending on the user preference) that the website disable either its own (first-party) or cross-site (third-party) tracking.[19] Since the advertising industry lacks a means of comprehensive self-regulation, the FTC believed that businesses could best respect consumers' tracking preferences through a simple system like DNT.[20] The response from industry-members was less than supportive.[21]

The release of the preliminary proposal by the FTC pre-empted the advertising industry's own attempts at a self-regulating, opt-out system.[22] This move by the FTC led browser developers to quickly engage with the DNT proposal and see whether they could be the first-movers on this new frontier.[23] Mozilla's Firefox became the first major browser to implement the DNT feature into their program.[24] Microsoft's Explorer[25] and Apple's Safari browser (among others) added support for the mechanism within months of the release of the preliminary report.[26]

While some third parties committed to honor these DNT preferences, even without

---

15. *See* FED. TRADE COMM'N, *supra* note 12, at 13 (discussing consumer education models).

16. *Id.* This third prong is essentially a mechanism for modernizing and refining the overly clunky, confusing, and legalese-filled privacy policies mandated by the FTC's notice-and-choice approach.

17. Tene & Polonetsky, *supra* note 10, at 327 (discussing renewed public interest in privacy).

18. DO NOT TRACK, http://donottrack.us (last visited Oct. 29, 2015).

19. *Id.* (discussing that tracking consent requests are used for both first and third party tracking.).

20. Angelica Nizio, *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*, 2014 U. ILL. J.L. TECH. & POL'Y 283, 296 (2014) ("[A] recent study shows that while companies committed to following [a] self-regulatory approach, there was still frequent non-compliance with providing consumers the option to opt out of behavioral tracking." In addition, one of the FTC's goals with the DNT system is "universal implementation," which is difficult to do with no uniform compliance standard.).

21. *See* Tene & Polonetsky, *supra* note 10, at 315–16 (citing a response from the Interactive Advertising Bureau which said that a federally proposed, sanctioned, and managed DNT system would essentially be a government-run, Ad-block system—something completely antithetical to the First Amendment).

22. *See* IAB, *infra* note 94 (describing the adoption of the Self-Regulatory Principles for Online Behavioral Advertising).

23. *See id.* (stating there is a "promot[ion] . . . of the 'Advertising Option Icon' and accompanying language, to be displayed within or near online advertisements or on Web pages where data is collected and used for behavioral advertising").

24. Julia Angwin, *Web Tool on Firefox to Deter Tracking*, WALL STREET J. (Jan. 24, 2011, 12:01 AM EST), http://www.wsj.com/articles/SB10001424052748704213404576100441609997236.

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

26. Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL STREET J. (Apr. 14, 2011, 12:01 AM EST), http://online.wsj.com/news/articles/SB10001424052748703551304576261272308358858?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748703551304576261272308358858.html.

existing enforcement or incentives to do so, the vast majority of both first- and third-party advertisers and data collectors have not.[27] One of the many industry objections was that behavioral targeting is a key component to the success of advertising networks and publishers.[28] Further, maintaining the current revenue source from behavioral advertising is essential in preserving the existence of free content and services.[29]

B. Draft Legislation

Following the FTC's preliminary report, the United States saw a flurry of activity from federal and state legislatures to protect consumers' privacy rights by creating a new regulatory system.[30] Though legislators and consumer rights groups pushed for industry regulation, none of the proposed bills have gotten any traction.[31] At the time of this writing all of the proposed bills remain un-passed.[32]

1. Do Not Track Me Online Act of 2011

The Do Not Track Me Online Act directed the FTC to promulgate regulations for "an online opt-out mechanism to allow a consumer to effectively and easily prohibit the collection or use of any covered information[33] and to require a covered entity[34] to respect the choice of such consumer to opt out of such collection or use."[35] The bill authorizes the FTC to enforce these regulations mainly through a random audit process.[36] In addition, the bill delegates limited authority to state attorneys general to bring civil suits on behalf of

27. *See Implementations*, DO NOT TRACK, http://donottrack.us/implementations (last visited Oct. 29, 2015) (listing third parties that have communicated a commitment to follow DNT); *see also* Rainey Reitman, *White House, Google, and Other Advertising Companies Commit to Supporting Do Not Track*, ELECTRONIC FRONTIER FOUNDATION (Feb. 23, 2012), https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track (stating that major industry-players had committed to supporting DNT by the end of 2012). This commitment to honor DNT has gone unfulfilled by the companies who vowed to support it. *Overview*, DO NOT TRACK, http://donottrack.us/ (last visited Oct. 29, 2015).

28. *See* Howard Beales, *The Value of Behavioral Targeting*, NETWORK ADVERTISING INITIATIVE, Dec. 16, 2009, at 1, 18, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf ("For the typical network, [Behavioral Advertising] accounted for just over 40[%] of total advertising revenue in 2009, with more than half of the total revenues going to publishers.").

29. *Id.* at 18.

30. *See* Josephine Liu, *Flurry of Privacy Bills Introduced in Congress; More to Come?*, INSIDEPRIVACY (June 17, 2011), http://www.insideprivacy.com/childrens-privacy/flurry-of-privacy-bills-introduced-in-congress-more-to-come/ (listing the various DNT, privacy, and data security bills proposed by Congress as of June 17, 2011).

31. *See* Brandon Sasso, *FTC Shows Little Interest in 'Do Not Track' Mandate*, THE HILL (Aug. 20, 2013, 8:27 PM EDT), http://thehill.com/policy/technology/317925-ftc-shows-little-interest-in-mandating-do-not-track (citing Rep. Brill, in acknowledging that "many people have given up on the industry talks ever producing a solution").

32. *See* Nizio, *supra* note 20, at 291 (explaining that "[b]ecause of the ongoing trouble with implementation, legislation has been reintroduced by various members of Congress").

33. Do Not Track Me Online Act of 2011, H.R. 654, 112th Cong. §2(3)(A) (2011), http://www.gpo.gov/fdsys/pkg/BILLS-112hr654ih/pdf/BILLS-112hr654ih.pdf. Covered Information defined as specific data that an individual transmits online. This includes websites accessed, data gleaned from consumer's browsing, unique identifiers (IP address, location, financial records, etc.).

34. *Id.* § 2(2). A Covered Entity is a person engaged in interstate commerce that collects or stores online consumer data.

35. *Id.* § 3(a).

36. *Id.* § 4(3).

consumers if non-compliance is discovered—though enforcement avenues beyond this procedure are not outlined in the bill.[37]

2. The Kerry/McCain Commercial Privacy Bill of Rights Act of 2011

Senators John Kerry and John McCain proposed the Commercial Privacy Bill of Rights Act, which sought to strike a compromise between business and consumer interests.[38] The Act moved away from the FTC's DNT mechanism and instead focused on informed consumer choice and industry transparency.[39] The legislation would require websites to explain their data collection practices, how they do it, and what happens to consumer data once collected.[40] The websites would then have to offer consumers a chance to opt out of data collection, and, for those who opt in, place restrictions on the types of data that are collected and how long the site can store it.[41] Furthermore, the Act tasked the FTC with creating a "safe harbor"[42] program to incentivize implementation of the program by exempting harbor-members from parts of the Bill.[43] Consumer advocates criticized the Act for its abandonment of a DNT mechanism and its reliance on the publically disparaged notice-and-choice model[44] that was already in place in most parts of the industry.[45]

3. Consumer Privacy Bill of Rights

In 2012, the Obama administration proposed the Consumer Privacy Bill of Rights.[46]

---

37. *Id.* § 5(a).

38. *See* Cecilia Kang, *Senators Introduce Internet Privacy Bill*, WASH. POST (Apr. 12, 2011), http://www.washingtonpost.com/blogs/post-tech/post/senators-introduce-internet-privacy-bill/2011/04/12/AFL0CjRD_blog.html (noting that Microsoft, Intel, and eBay support this legislation).

39. *See id.* (quoting John Kerry in saying that the DNT mechanism was not included in the bill because "it didn't seem to fit in our ability to get a balance for consumer and industry support").

40. *Id.*

41. *See id.* (explaining that while data use would be restricted to "only that which is necessary to process . . . a transaction or deliver a service," the bill would give discretion to internet firms to use data for "research and development" and retain that data for "a reasonable period of time").

42. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 501 (1st Sess. 2011). According to the Bill, the safe harbor would allow the FTC to appoint a non-governmental organization (NGO) to oversee a separate, voluntary program capable of achieving the same protections to consumer data as enumerated in the Act. Incentives for enrolling in the program include allowing safe harbor participants to design their own, individual procedures for compliance. By doing so, participants would be exempt from any provision of Title II (requiring providing consumers with notice and transparency of their program) and Title III (mandating strict data security and limits on data collection) of the Bill's requirements.

43. *Id.* at 41.

44. FED. TRADE COMM'N, A PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS 40 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf; *see also supra* note 16 and accompanying text (stating that the new "framework requires increased transparency so that users can easily understand the information in a given business' stated privacy policies" to modernize the unrefined notice-and-choice approach).

45. *See* Jacqui Cheng, *Consumer Groups Skeptical About New Kerry-McCain Privacy Bill*, ARSTECHNICA (Apr. 12, 2011, 3:27 PM CDT), http://arstechnica.com/tech-policy/2011/04/consumer-groups-skeptical-about-new-kerry-mccain-privacy-bill (acknowledging that "the bill relies too much on the 'notice and choice' model that already exists at most companies").

46. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 11–22, WHITE HOUSE (Feb. 2012), http://www.whitehouse.gov/sites/

The proposal stated that consumers have the right to individual control over their data and how companies use it.[47] Furthermore, the proposal outlined consumer rights to transparency in privacy policies and security practices, as well as the right to expect that companies will collect or not collect consumer information in accordance with their stated tracking preferences.[48] The proposal also included expectations of secure and responsible handling of collected consumer data, consumer access to personal data, reasonable limits on collected data, and accountability by companies through providing measures showing they adhere to the Consumer Privacy Bill of Rights.[49] While Internet companies such as Mozilla, Google, Microsoft, and AOL promised to provide a DNT mechanism to facilitate participation in the Obama Administration's proposed guidelines,[50] there are no means of enforcing those guidelines without legislation granting the FTC authority to act on violations.[51] Consumer rights groups strongly supported the move and asserted that "industry self-regulation . . . has failed to inform or protect consumers."[52] On the other hand, industry groups oppose new legislation, stating their preference for the United States to enforce existing laws that address the misuse of consumer data.[53] Furthermore, they argue that regulations based on "theoretical potential harms" would create an increase in both compliance costs and uncertainty in the advertising and data-brokering industry.[54]

C. "Successful" Legislation Abroad: EU and The Right to be Forgotten

While data privacy laws struggle to gain traction in the United States, the European Union (EU) employs an aggressive privacy stance through Directive 95/46[55] (the Data Protection Directive or Directive).[56] The dual purpose of the Data Protection Directive is to preserve the rights of citizens to protect their personal data and "facilitate the free flow of personal data between and within EU member states."[57] Meeting these two goals requires firms to receive affirmative consent from individual consumers prior to using, processing, or storing those consumers' personal data.[58]

In addition to consent, the Directive also mandates that consumers receive timely notice of the identity of their "data controller," as well as information regarding the

---

default/files/privacy-final.pdf.

47. *Id.*

48. *Id.*

49. *Id.*

50. *Yahoo to Implement 'Do Not Track' Mechanism*, WALL STREET J. VIDEO (Mar. 29, 2012, 1:42 PM), http://www.wsj.com/video/yahoo-to-implement-do-not-track-mechanism/512A1484-8AA7-4A39-BA14-7D64E4D10B43.html.

51. Nizio, *supra* note 20. While the FTC is given authority to adopt regulations for industries to follow to achieve consumer privacy, the new legislation would enhance that authority by giving the FTC the power to specifically target and regulate behavioral advertising as a deceptive consumer practice.

52. Wendy Davis, *Advocates, IAB Weigh In On Privacy 'Bill of Rights'*, MEDIAPOST (Aug. 5, 2014, 8:10 PM), http://www.mediapost.com/publications/article/231499/advocates-iab-weigh-in-on-privacy-bill-of-rights.html.

53. *Id.*

54. *Id.*

55. Council Directive 95/46, art. 1–4, 1995 O.J. (L 281) (EC).

56. Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. & TECH. 2, 4 (2011).

57. *Id.*

58. *Id.*

recipients of that data, and whether the collected data is subject to a "right of access" by the consumer to rectify or remove the data.[59] Unlike the various incarnations of U.S. law, the Directive makes no use of a DNT-style mechanism to track consent. Instead, the Directive requires that websites notify users any time the site requests to place tracking cookies on a user's computer, thereby allowing users the opportunity to opt in or opt out of tracking by individual websites.[60]

Behavioral advertising adds an interesting wrinkle to the Directive's notion of informed consumer consent. While the Directive makes essential the need for "free and informed consent" by a consumer prior to tracking, the definition of consent varies from member state to member state.[61] This discrepancy has led to a push in the EU to revise its privacy policies and implement a DNT-style system to supplement the existing framework and better facilitate consent that is both clear and comprehensive across all member states.[62]

III. ANALYSIS

The state of DNT is currently in limbo.[63] Both consumer privacy advocates and free-market hawks are engaged in a scope-defining arms race—advancing varying ideas of what DNT should mean, whether and how it should be implemented, and whether it is even a viable means of advancing the public interest. This Part discusses the effect that various interpretations of DNT would have on the future of consumer privacy interests and the state of a—for now—cost-free Internet experience.

A. "Do-Not-Track" by Default

While many of the DNT proposals have called for tracking-preference to be a product of active, conscious consumer choice, privacy rights groups have strongly expressed that a preference against tracking should be the default for consumers unless chosen otherwise.[64] Microsoft was one of the first industry-members to state a willingness to honor preferences received through a default preference mechanism.[65] Microsoft set itself apart from its

59. *Id.*

60. *Id.* at 9.

61. Kirsch, *supra* note 56, at 15.

62. *Id.*

63. *See* Ed Bott, *Why Do Not Track is Worse than a Miserable Failure*, ZDNET (Sept. 21, 2012), http://www.zdnet.com/why-do-not-track-is-worse-than-a-miserable-failure-7000004634/ (summarizing that, though from a consumer's perspective the concept and purpose of "Do Not Track" is clear, the data-collecting companies proposing the standard seem intent on making sure it does nothing at all).

64. *See* Peter Bright, *Microsoft Sticks to its Guns, Keeps Do Not Track on by Default in IE10*, ARSTECHNICA (Aug. 7, 2012, 8:00 PM CDT), http://arstechnica.com/information-technology/2012/08/microsoft-sticks-to-its-guns-keeps-do-not-track-on-by-default-in-ie10/ (stating that members of the Congressional Privacy Caucus and The European Commission's director-general for Information, Society, and Media had expressed support for Microsoft's rollout of a default DNT preference with its 2012 release of Internet Explorer 10); *see also* TRACKING PROTECTION WORKING GROUP, TRACKING PREFERENCE EXPRESSION (DNT) § 4 (2015), http://www.w3.org/TR/tracking-dnt/ (stating that the key to the notion of a stated tracking preference is that "the signal sent MUST reflect the user's preference, not the choice of some vendor . . . or . . . mechanism outside the user's control").

65. *IE9 and Privacy: Introducing Tracking Protection*, IEBLOGS (Dec. 7, 2010, 12:10 PM), http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx (explaining the implementation of Microsoft's privacy mechanism).

contemporaries by adopting a default setting in Internet Explorer 10 that automatically opted out of behavioral tracking.[66] The pushback from the advertising industry was almost immediate.[67] It took only one week from the time that Microsoft's new setting was announced, for the World Wide Web Consortium (W3C)[68] to disseminate an updated draft of specifications; the centerpiece being that the user must state any tracking preferences—as an active, conscious choice—for those preferences to be recognized.[69] Regardless of the response, Microsoft stood by its decision to include the default opt-out preference.[70]

While opposition from the industry was vocal,[71] arguments from legislators and consumer advocates in favor of a default opt-out standard were favored by concerns over both consumer privacy as well as economic efficiency.[72] In his article on a default opt-out tracking standard, Professor Fairfield argues that allowing a consumer to state his tracking preferences for every particular site visited increases transacting cost both individually as well as in the aggregate, therefore making it a practice to avoid from a cost-efficiency standpoint.[73] As the threats to privacy multiply, so too must privacy enhancements.[74] Fairfield argues that in order for a DNT mechanism to be effective, it must not be adopted as an industry standard (and especially not adopted as legislation), but rather must be delivered to consumers "like any other software tool."[75]

Though there are camps backing the default opt-out mechanism as an effective tool for consumers to state their tracking preferences, many in the industry oppose this approach.[76] One argument against a default opt-out approach is that such a policy could have a fundamental impact on the Internet economy.[77] If tracking preferences actually

66. *See* Bright, *supra* note 64 (stating that advertisers "had a fit" with the fact that by making the end user manually opt in to behavioral tracking, Microsoft had, by default, made a move to cut off the advertising industry from a significant number of web users).

67. *Id.*

68. WORLD WIDE WEB CONSORTIUM, http://www.w3.org/ (last visited Oct. 29, 2015). The W3C is an international standards setting organization, whose work is dedicated to furthering the growth of the internet. It is also the lead-member of the industry collective in charge of creating DNT specifications and proposing modes of implementation of enforcement.

69. *See* Bright, *supra* note 64 (proposing that by sticking to its position, Microsoft might create an environment where tracking preferences are widely stated but largely ignored by even those advertisers who say they will comply with DNT).

70. *Id.*

71. Due, primarily, to the fact that it would effectively stifle advertisers' free and instantaneous access to consumer data. This point is further discussed below.

72. Fairfield, *supra* note 9, at 611 (arguing that more consumer privacy choice leads to greater transaction costs).

73. *See id.* at 606 (stating that while reading one privacy policy may not be all that harmful or time-consuming for an individual, reading and making a conscious choice about hundreds of websites is an efficiency cost that is too great to the consumer to justify).

74. *Id.*

75. *See id.* at 607, 619–20 (stating further that the idea of "privacy by design" does not automatically solve the issue of delivery to consumers—Facebook's overly cumbersome—although integrated—privacy suite is an example that the choice needs to be more efficiently presented to consumers in order for it to be meaningful and effective).

76. *See DAA Statement on DNT Browser Settings*, BUSINESS WIRE (Oct. 9, 2012, 8:30 AM EDT), http://www.businesswire.com/news/home/20121009005980/en/DAA-Statement-DNT-Browser-Settings#.VEm-qhbIrIs (stating that "[m]achine-driven Do Not Track does not represent user choice; it represents browser-manufacturer choice" and that a default mechanism does little in terms of meaningfully giving consumer's the power of control over their personal data).

77. Benjamin Strauss, *Online Tracking: Can the Free Market Create Choice Where None Exists?*, 13 CHI.-

became enforceable, and site-owners complied with those preferences (even if expressed by default), the sudden lack of ad revenue collected from behavioral tracking could end incentives for these owners to offer free content.[78] One commentator notes that a default system may unnecessarily end behavioral advertising entirely, even though behavioral advertising enables a type of online experience that is valuable to consumers through data collection, which many consumers do not mind.[79]

The Digital Advertising Alliance (DAA)[80] also came out against the default standard, for reasons of both consumer choice and the drastic effects it could have on the industry as a whole.[81] The DAA and its members claimed that proposals to set DNT to default undercut the progress of effective self-regulation and create an environment where the advertiser's choice to honor or ignore a DNT signal[82] is increasingly unpredictable.[83] Interestingly, in 2013 the DAA crafted a new proposal on DNT specifications—one that proposed that a consumer's DNT signal *should* be set to a default, albeit to a default of "I wish to be tracked."[84]

B. Industry Self-Regulation

While industry-members promised to provide and comply with a DNT mechanism by the end of 2012,[85] that pledge went (and is still going) unfulfilled.[86] Currently, there are no means to specifically enforce DNT guidelines without legislation granting the FTC authority to regulate online consumer privacy.[87] In light of this failure, Senator John Rockefeller, author of the "Do Not Track Online Act of 2011," blasted the industry for

KENT J. INTELL. PROP. 539, 568 (2014).

78. *Id.*

79. *Id.*; *see also* Tim Worstall, *Microsoft Sticks With Do Not Track Default: And Boy Are The Advertisers Angry*, FORBES (Oct. 3, 2012, 1:09 PM), http://www.forbes.com/sites/timworstall/2012/10/03/microsoft-sticks-with-do-not-track-default-and-boy-are-the-advertisers-angry/ (stating that a default setting that "most people will stick with, thus means that all of the complicated work that the advertising industry [does] to increase the performance of internet advertising becomes . . . irrelevant").

80. *About the Digital Advertising Alliance*, YOUR ADCHOICES, http://www.yourAdChoices.com/aboutus.aspx (last visited Oct. 29, 2015). The DAA is a consortium of the leading national advertising and marketing trade groups that deliver effective, self-regulatory solutions to online consumer issues. It was a member of the W3C's 110-member tracking protection working group (TPWG). It abandoned the project in 2012, after two and a half years of membership. Katy Bachman, *Digital Advertising Alliance Exits Do Not Track Group: Development Could Renew Calls for Privacy Laws*, ADWEEK, (last visited Oct. 29, 2015), http://www.adweek.com/news/technology/digital-advertising-alliance-exits-do-not-track-group-152475.

81. *See* Katy Bachman, *Take That, Microsoft: Digital Ad Community's Final Word on Default Do Not Track*, ADWEEK (Oct. 9, 2012, 10:17 AM), http://www.adweek.com/news/technology/take-microsoft-digital-ad-communitys-final-word-default-do-not-track-144322 ("Allowing browser manufacturers to determine the kinds of information users receive could negatively impact the vast consumer benefits and Internet experiences delivered by [industry] participants and millions of other websites that consumers value.").

82. A DNT signal communicates either a preference to opt in or opt out.

83. *See* Bachman, *supra* note 81 (stating that the DAA will not honor default DNT signals, they will not penalize member-firms for ignoring them, and that the issue affects the capability of the DAA to give guidance to its member's on how to proceed with handling DNT signals).

84. *Draft Framework for DNT Discussions Leading Up to Face-to-Face*, W3C (Apr. 29, 2013), http://lists.w3.org/Archives/Public/public-tracking/2013Apr/att-0298/one_pager_framework_as_distributed.pdf.

85. *Yahoo to Implement 'Do Not Track' Mechanism*, *supra* note 50.

86. Gross, *infra* note 99.

87. *See* Nizio, *supra* note 20, at 303 (stating that uniform implementation could be achieved only if Congress granted the FTC authority to hold industry members accountable).

"dragging its feet" and reiterated his position for the FTC to have power to regulate and enforce a comprehensive tracking policy that would cover consumers "across the Internet."[88]

Members of the advertising industry are opposed to giving the FTC enforcement power to a DNT standard via legislation.[89] One of the primary criticisms of DNT, from the industry perspective, is that it threatens the existing online ecosystem where consumers allow sites and ad networks to collect their data in exchange for open access to many free applications and services.[90] Mike Zaneis, general counsel for the Interactive Advertising Bureau (IAB) (an industry group and DAA member), commented that by doing away with relevant behavioral advertising, we "make the Internet less diverse, less economically successful, and frankly, less interesting."[91] Privacy, one industry article notes, "requires the active management of trade-offs."[92]

Advertisers have responded to the push for enhanced online privacy initiatives in varying ways. Some—such as the members of the W3C—have worked to create a coalition to manufacture a DNT regime that satisfies both the advertising industry and consumer rights organizations.[93] Others—like the IAB and the Network Advertising Initiative (NAI)—have supported the notion of self-regulation through enhanced consumer choice.[94] The latter approach to self-regulation involves an Advertising Options Icon (AdChoices Icon) that allows consumers faced with targeted ads to click on an ad, get information on how their data is being used, and then choose to opt-out of the particular advertisement.[95]

In regard to a W3C-proposed, self-regulated, DNT mechanism, proponents have stated that the willingness of industry members to comply with the notion of DNT is an encouraging sign that the market is adapting to consumer preference in the area of online privacy.[96] In a recent article, Benjamin Strauss proposed that one way to encourage participation in a self-regulatory DNT program would be to infuse incentives—both on the part of the consumer as well as the advertiser—in the decision to opt in or out.[97] Strauss,

---

88. *See* Gross, *infra* note 99 (explaining further his skepticism with the belief that "companies with business models based upon the collection and monetization of personal information will voluntarily stop these practices if it negatively affects their profit margins").

89. Davis, *supra* note 52.

90. Natasha Singer, *Do Not Track? Advertisers Say 'Don't Tread on Us'*, N.Y. TIMES (Oct. 13, 2012), http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html.

91. *Id.*

92. *See* Colin O'Malley, *Self-Regulation Solves the Do Not Track Problem*, IAB (Feb. 23, 2011, 4:57 PM), http://www.iab.net/iablog/2011/02/self-regulation-solves-the-do-.html ("DNT relies on the false promise of a privacy 'on-off' switch, and encourages the masses to make a blunt decision, without context, with massive negative impact on industry that will circle back to the consumer.").

93. *See Tracking Protection Working Group*, W3C, http://www.w3.org/2011/tracking-protection/ (last visited Oct. 29, 2015) (describing its mission to "improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking . . . . The group seeks to standardize the technology and meaning of Do Not Track . . . .").

94. *Major Marketing / Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising*, IAB (Oct. 4, 2010), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410.

95. *Id.*

96. Strauss, *supra* note 77, at 570.

97. *See id.* (suggesting that Google and other service providers could incentivize consumer-consented tracking by maintaining free access to offered services (mail, docs, calendar, etc.) while charging fees to those consumers who choose to opt out. This would force the consumer to make a value judgment, and therefore, would lead to a more informed and personally-tailored internet experience for the consumer).

among others, also suggests that by placing the power in the hands of the consumer (as opposed to the legislature), they force advertisers to reform their collection practices to respond to consumer demands and preferences.[98]

Consumer rights groups,[99] the FTC,[100] and members of Congress[101] have been vocal in their opposition to a solely self-regulated privacy and tracking scheme, as well as to alternative proposals such as the AdChoices Icon.[102] In 2012, then-Chairman of the FTC, Jon Leibowitz, suggested that the industry's opposition to DNT regulation could backfire—adding incentive for frustrated users to opt out and creating a race amongst browsers to see "who can be the most privacy-protective."[103] Senator John Rockefeller, in a 2012 letter to Leibowitz, expressed displeasure with the current state of DNT, suggesting that self-regulation "for the purposes of consumer privacy protection" had failed.[104] Consumer watchdog agencies largely support Rockefeller's position and remain supportive of legislation that would take the regulatory power out of the hands of the industry and place it with the FTC.[105]

The industry's own attempt at creating a tracking preference and self-compliance program—the AdChoices Icon—has received not-so-glowing reviews in terms of effectiveness.[106] Criticizing industry pronouncements of wide-spread consumer adoption, opponents point to a research study showing that consumer awareness of the icon's existence and basic function has teetered around six percent in the three years of the AdChoices Icon's availability.[107] Regardless of the progress (or lack-thereof) of AdChoices and similar initiatives, consumer groups still push for uniform acceptance by the advertising industry of DNT standards (either by self-regulation or legislation).[108]

C. Mirroring Existing Privacy Laws: Would Following the EU's Lead Be Effective To

98. *Id.* at 540; *see also* Timothy J. Shrake II, *Who's Following You: The Federal Trade Commission's Proposed "Do Not Track" Framework and Online Behavioral Advertising*, 36 S. ILL. U. L.J. 383, 404 (2012) (positing that "[i]f companies follow consumer wishes then no problems should arise").

99. Grant Gross, *Senator Rips Self-Regulatory Do-Not-Track Efforts*, PCWORLD (Apr. 24, 2013, 2:47 PM), http://www.pcworld.com/article/2036323/senator-rips-selfregulatory-donottrack-efforts.html.

100. Brad Reed, *FTC Chair Slams Advertisers' 'Self-Regulated' Do Not Track System*, BGR (Apr. 18, 2013, 8:55 PM), http://bgr.com/2013/04/18/online-advertisers-do-not-track-criticism-447808/.

101. Strauss, *supra* note 77.

102. Kate Kaye, *Study: Consumers Don't Know What AdChoices Privacy Icon Is*, ADAGE (Jan. 29, 2014), http://adage.com/article/privacy-and-regulation/study-consumers-AdChoices-privacy-icon/291374/ (discussing AdChoices, a program launched by a coalition of the largest advertising industry groups, that enables consumers who click on its icon to opt-out of targeted ads).

103. Singer, *supra* note 90.

104. *See* Letter from John D. Rockefeller, Chairman, Senate, Sci. and Transp. to Jon Leibowitz, Chairman, Fed. Trade Comm'n, (Oct. 3, 2012), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id= fab9be53-8418-44db-b345-79220cd61f3b (stating that even though the DAA had pledged to honor DNT signals, their pledge was so "riddled with exceptions" as to render DNT compliance "meaningless").

105. Katy Bachman, *Digital Ad Biz to Defend Self-Regulation at Do Not Track Hearing Privacy Groups Complain Progress is Too Slow*, ADWEEK (Apr. 22, 2013, 4:32 PM EDT), http://www.adweek.com/news/technology/digital-ad-biz-braces-do-not-track-hearing-148816.

106. Kaye, *supra* note 102 (finding in 2014, that three years after its launch consumers were aware of the industry's opt-out program).

107. *Id.* The study also showed that the percentage of consumers who clicked the icon but still were unaware that they had the option to opt out of further tracking rose from 14% in 2011 to 27% in 2013.

108. Singer, *supra* note 90.

Move Policy Forward in the United States?

With a regulatory system already in place, the EU's online privacy environment seems to be both a literal and figurative ocean away from the environment here in the United States. At the same time, however, the EU is grappling with the issue that the United States is facing—what to do with the rise of targeted, behavioral advertising. For the past five years, legislators and consumer groups have pushed for the Directive to incorporate a near-identical form of the DNT mechanism as has been proposed in the United States.[109] Through the Directive, users have the right to consent or refuse to consent to the use of their data in behavioral advertising.[110] Proposals of a DNT mechanism to more easily facilitate that consent have run into—not surprisingly—similar roadblocks as in the United States.[111] Concerns over implementation, compliance, enforcement, and lack of industry support have plagued—and all but halted—progress on a DNT approach.[112]

Alternative approaches to achieving consumer-control of data have not fared much better.[113] Self-regulatory initiatives by UK industry collectives—focusing on creating a set of best practices—present a rigid dichotomy between consumer interests and the importance of behavioral advertising.[114] With a lack of approaches in position to make a meaningful difference in the EU's approach to behavioral tracking, the EU is in much the same position as the United States—still searching for an effective way to respond to consumer preferences.

IV. RECOMMENDATION

One of the hallmarks of the ongoing debate surrounding consumer privacy and DNT legislation is the concept of choice. Consumer rights groups advocate for legislation because they want an enforcement mechanism to ensure that companies respect and honor consumer tracking preferences. Industry groups actively chastise Microsoft for releasing a browser with settings that make the choice *for* consumers—while coincidentally harming industry interests. Granting enforcement authority to the FTC through legislation, as we have seen, has gotten little meaningful traction.[115] Though this concept has been kicked around at least in some form for the past seven years, there is little indication—especially with a more anti-regulatory majority taking control in the 113th Congress—that substantial change will happen soon.

Attempts at industry self-regulation as a viable alternative to enforcement have been largely unsuccessful. This is highlighted by the fact that the industry collective in charge of coming up with a plan to deal with and possibly implement DNT mechanisms could not

109. Richard Beaumont, *Do Not Track Gets Thumbs Down From EU*, OPTANON (June 12, 2014), http://www.cookielaw.org/blog/2014/6/12/do-not-track-gets-thumbs-down-from-eu/.

110. Kirsch, *supra* note 56, at 45–46.

111. Beaumont, *supra* note 109.

112. *Id.* Many of the specifications of the proposed EU DNT standard fail to comply with the Directive's own cookie and consent laws.

113. *See* Kirsch, *supra* note 56, at 46–48 (stating that the industry has had 15 years since the adoption of the Directive to engage in meaningful self-regulation and have failed). Kirsch outlines an unrealistic alternative proposal that consumers should be forced to consent or refuse consent to every tracking cookie they encounter.

114. Kirsch, *supra* note 56, at 31.

115. *See* Angwin, *supra* note 31 and accompanying text (noting that Mozilla's Firefox became the first major browser to implement the DNT feature into their program).

even maintain the support and cohesion of its own members for longer than a two-year period.[116] Without the force of legislative authority, it is unlikely that other approaches can adequately and efficiently protect consumer interests over the long term. However, with the difficulty in building consensus on the policy of tracking itself, a realistic (or timely) option should not rely on legislation alone.[117] In order to enable consumer education and conscious choice about tracking preferences—which seems to be the sticking point for many approaches to solving the DNT issue—consumers must have instant, clear access to information about the actual third parties that track them on a given website.

A default DNT standard—much like the one proposed by consumer-rights groups and implemented by Microsoft's Internet Explorer browser—would most certainly deprive consumers of an Internet experience that they are used to and that works for them. On the other hand, setting a default to permit tracking might allow the user to seamlessly continue his browsing experience, but it does not really solve the data-control problem. We must give consumers the tools they need to make informed choices about what type of information is taken from their browsing history, what is done with that information, and who is doing it. By doing this, we can create an environment where consumers get used to tailoring their online experience and can be in a better position to "vote with their feet." Through a combination of the FTC's proposed DNT standards, as well as in-browser tools that keep the consumer aware of what data is being collected (and if it is being collected at all) on a site-by-site basis, consumers will have a meaningful say in a decision that affects both their autonomy over personal data as well as the consistency and effectiveness of their browsing experience.

A. Free(ish)-Market Foundation

In lieu of legislative enforcement, browsers and industry members would have to get on board with one simple reality: the issue of tracking is not going to go away. There are already tools in the way of add-ons, browser settings, and even the arguably ineffective AdChoices program[118] that scratch the surface but fall short of what is necessary to get the broader public engaged. Instead of burying these tools in the settings section of a browser toolbar or relying on particularly tech and privacy conscious consumers to customize their experience[119] or even making their presence so unclear that they are largely ineffective,

---

116. Kate Kaye, *DAA Leaves (And Cripples) Do Not Track Group*, MARKETING MAG (Sept. 17, 2013), http://www.marketingmag.ca/media/daa-leaves-and-cripples-do-not-track-group-88861. In 2013, and after two years of admittedly "no progress" on privacy issues, the DAA split from the W3C's Tracking Preference Working Group in order to propose a competing, more self-governing solution to the consumer tracking issue.

117. However, granting enforcement authority to an agency such as the FTC would be the most feasible way to ensure some level of uniform regulation and enforcement. The fact that the current political landscape seems less than receptive to grant this regulatory power anytime soon is irrelevant. Without some legal enforcement mechanism, there are limits to what the free market alone can accomplish.

118. *See* Wendy Davis, *Study: Web Users Don't See AdChoices Icon*, MEDIAPOST RAW (Nov. 13, 2012, 8:39 AM), http://www.mediapost.com/publications/article/187164/study-web-users-dont-see-AdChoices-icon.html (stating that while the AdChoices icon is present in one trillion ad impressions per month, studies show that only one in five consumers notice the icon and many users mistakenly believe that clicking on the icon would actually create pop up ads).

119. These are two of the many reasons that the DAA and other industry-members gave for why there shouldn't be a blanket opt out by default. With them at least recognizing that issue, it might be more feasible for them to get on board with this approach.

these tools need to be front, center, and understandable. To that end, I recommend the major browsers implement a variation of the DNT mechanism typically buried in the browser-settings by integrating that mechanism into the browser's permanent toolbar. The toolbar would indicate: (1) whether the currently visited website pledged to honor the FTC's proposed tracking preferences, (2) agencies that are tracking or attempting to track information on a given website, (3) the typical use of the data being collected, and (4) how opting in or out affects the user's experience.

If presented in this way, the user is not bombarded with information that they will likely ignore and is aware the information is at his fingertips should he desire to customize his experience further. Existing add-on programs, such as "Blur," offer a variation of this approach that actively blocks the tracking cookies sent by websites as opposed to sending a statement of the user's tracking preference.[120] After broad adoption of this toolbar-based notice, users will be able to identify which choices affect what part of their browsing experience as well as which sites disregard their preferences altogether.

B. FTC in Support Position

With consumers having the information they need to make informed decisions about tracking preferences and browsing habits, they would be able to more effectively browse if they know that certain sites don't honor their preferences. However, because certain sites have a great deal of market share in certain sectors of the Internet (i.e., Google, Amazon, Facebook, etc.), FTC enforcement would be the most effective means for punishing the entities that would otherwise be practically immune from threats of consumer migration. The current FTC approach to enforcing DNT would likely be the best way to move forward. The only difference between its failure to gain traction now and the possible success of the approach in the future is the variable of broad consumer support and engagement. With voters constantly making decisions affecting their privacy, they will be the missing ingredient of leverage needed to boost support both in the legislature as well as within the industry.

V. CONCLUSION

Though a great deal of fervor has occurred surrounding the need for enhancements to our online privacy rights, very little has been done to actually increase the amount of control that we have over our own information. Seemingly successful attempts at policy overhauls abroad still lack the means to deal with the invasiveness of online advertising. The currently unrestricted nature of data collection and dissemination adds even more wrinkles to an otherwise complicated environment.

If meaningful change will occur, it cannot happen without full participation by both the consumer and the industry. In order for the consumer to become engaged, however, they need to know that their voices are being heard and their preferences honored. While the free-market choice available to consumers *is* theoretically available, the realities of our increasingly online lives makes this less and less likely without the enforcement muscle that legislation and even segments of the private sector can provide.

120. The approach of actively blocking outside cookies is problematic from an industry standpoint, simply because it is probably the strongest pro-consumer approach you can have other than a default opt-out mechanism. Realistically, concessions will have to be made in order to have industry participation in the program.