Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 7 Article 2

Fall 2013

Do-Not-Track as Default

Joshua A.T. Fairfield
Washington & Lee University School of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Do-Not-Track as Default

Joshua A.T. Fairfield

September 2013 VOL. 11, NO. 7

Volume 11, Number 7 (September 2013)
Northwestern Journal of Technology and Intellectual Property

Do-Not-Track as Default

By Joshua A.T. Fairfield*

Do-Not-Track is a developing online legal and technological standard that permits consumers to express their desire not to be tracked by online advertisers. Do-Not-Track has the ability to change the relationship between consumers and advertisers in the information market. Everything will depend on implementation. The most effective way to allow users to achieve their privacy preferences is to implement Do-Not-Track as a default feature.

The World Wide Web Consortium's (W3C) standard setting body for Do-Not-Track has, however, endorsed a corrosive standard in its Tracking Preferences Expression (TPE) draft. This standard requires consumers to set their privacy preference by hand. This "bespoke" standard follows in a long line of privacy preference controls that have been neutered by increased transaction costs.

This article argues that privacy controls must be firmly in consumers' hands, and must be automated and integrated to be effective. If corporations can deprive consumers of privacy through automated End User License Agreements or Terms of Service, while consumers are constrained to set their privacy preferences by hand, consumers cannot win. Worse, the TPE bespoke standard is anticompetitive. Already, browsers like Microsoft's Internet Explorer 10 (IE10) will launch with default Do-Not-Track enabled. But the TPE bespoke standard offers advertisers a free pass to ignore the Do-Not-Track flags that will be set by IE10 and prohibits other browsers from offering automatic, integrated, and therefore useable privacy features.

"Once they notice you, Jason realized, *they never completely close the file.* You can never get back your anonymity."

–Philip K. Dick, *Flow My Tears, the Policeman Said*

---

* © 2013 Joshua A.T. Fairfield. Professor of Law, Washington & Lee University School of Law. The Author would like to thank the Fulbright Commission and the Max Planck Institute for Research on Collective Goods for support during the drafting of this piece. Thanks to James Grimmelmann for comments and suggestions. The Author would like to thank Michael Bombace, Jill Nyhof, Joshua Laguerre, Hannah Shtein, and Matthias Kaseorg for important research assistance. All errors, opinions, and errors of opinion are the Author's.

I. INTRODUCTION

¶1 A common Internet meme is that privacy is dead.[1] It is more accurate to state that it has been buried. Privacy features exist, but they are left inactive by default and buried deep in programs or on websites for only a few to find and use.[2] This article asks whether a recent and promising pro-privacy feature will suffer the same fate.[3]

---

[1] *See* Michael J. Kasdan, *Is Facebook Killing Privacy Softly? The Impact of Facebook's Default Privacy Settings on Online Privacy*, 2 N.Y.U. INTELL. PROP. & ENT. LAW LEDGER 107 (2011) ("In the age of instantaneous sharing of information on Facebook, it is fair to ask whether privacy is dead or dying, and whether online social networks like Facebook are killing it."); *see also* Jared Newman, *Google's Schmidt Roasted for Privacy Comments*, PCWORLD (Dec. 11, 2009, 9:06 AM), http://www.pcworld.com/article/184446/googles_schmidt_roasted_for_privacy_comments.html (quoting Schmidt as stating, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time . . . ."); *Private Lives? Not Ours!*, PCWORLD (Apr. 18, 2000, 12:00 AM), http://www.pcworld.com/article/16331/article.html ("'You have zero privacy anyway,' Sun Microsystems' CEO Scott McNealy said last year. 'Get over it.'"). *But see* BRIAN X. CHEN, ALWAYS ON 188–89 (2011) (arguing that privacy is more dynamic and has changed given technological developments); Nick Bilton, *Privacy Isn't Dead. Just Ask Google+*, N.Y. TIMES, July 18, 2011, http://bits.blogs.nytimes.com/2011/07/18/privacy-isnt-dead-just-ask-google/ (outlining how Google focused on privacy concerns in Google+ after learning from Facebook's experience relating to privacy concerns).

[2] Pedro G. Leon et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 589, 589, 597 (2012), *available at* http://cups.cs.cmu.edu/rshay/pubs/CHI2012-opt-out-usability.pdf (presenting the results of a 45-participant study "investing the usability of tools to limit online behavioral advertising" and concluding that "[n]one of the nine tools . . . tested empowered study participants to *effectively* control tracking and behavioral advertising according to their personal preferences" (emphasis added)).

[3] *See* Stephen Shankland, *Apache Web Software Overrides IE10 Do-Not-Track Setting*, CNET (Sept. 7, 2012, 9:34 AM), http://news.cnet.com/8301-1023_3-57508351-93/apache-web-software-overrides-ie10-do-not-track-setting/ ("Apache, the most commonly used software to house Web sites, will ignore Microsoft's decision to disable ad-tracking technology by default in Internet Explorer 10."). *But see* Dan Goodin, *Apache Webserver Updated to Ignore Do Not Track Settings in IE 10*, ARS TECHINCA (Sept. 10, 2012, 3:22 PM), http://arstechnica.com/security/2012/09/apache-webserver-updated-to-ignore-do-not-track-

¶2 The feature, called Do-Not-Track (DNT), could potentially change the balance of power between consumers and corporations in the U.S. data marketplace.[4] Until recently, debate over Do-Not-Track focused on whether it would be implemented. Recent reports from the Federal Trade Commission (FTC), stakeholder statements at Senate hearings, and drafts from industry and standard-setting groups all indicate a growing consensus that some form of Do-Not-Track will be implemented.[5]

¶3 This article asks a central follow-up question about implementation: whether a consumer must set a Do-Not-Track flag by hand, or whether she may choose automatic, pre-packaged software that sets the flag for her. The article engages both industry arguments and the World Wide Web Consortium's (W3C)[6] Tracking Protections Working Group (TPWG) standard on Tracking Preference Expression (TPE), which requires that such a flag must be set by hand, without automation, in order to be enforceable or effective.[7] This article refers to the by-hand requirement of the TPE as the "bespoke" Do-Not-Track requirement,[8] and contrasts it with the norm for computer

---

settings-in-ie-10/ ("Critics of the Apache update contend Microsoft's Do Not Track implementation . . . is in compliance with the standard. A screen that is displayed when a user first uses the operating system offers two choices: Express settings and a more detailed Customized settings. The same screen explicitly states that choosing the Express option will turn on Do Not Track.").

[4] *Compare* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1648 (2011) ("Central to the issue of **consent** is the possible failure of the users to adequately understand the consequences of their **consent**—or to recognize that they are consenting to anything at all."), *and* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 601 (2006) ("If a person does not know about the possibility of changing an option or the ramifications of each choice, then a default setting is equivalent to a fixed setting."), *and* Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 292 (2012) ("Recently, Jonathan Mayer of Stanford University found that Google and other network advertisers . . . found a way to circumvent . . . cookie blocking. The method used by Google was particularly brazen—it opened a webpage invisible to the user and used a program to simulate the user clicking on it."), *and id.* at 295 ("[O]n a basic level, consumers' manifestations of choice should not be circumvented. . . . If advertisers wished to condition access to services on tracking, they could. But to do so, they would have to have some dialogue with the consumer, rather than resorting to sneaky technical methods to obscure the tracking."), *with* James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 5 (2005) ("If consumers are aware of their privacy concerns and deem privacy important, they are more likely to take steps to protect their own interests—for example, avoiding firms that might compromise their privacy interests and frequenting the ones that are more likely to protect them."), *and Do Not Track: Universal Web Tracking Opt Out*, http://donottrack.us/ (last accessed Sept. 3, 2012) [hereinafter *Do Not Track Us*] ("[D]o Not Track provides users with a single, simple, persistent choice to opt out of third-party web tracking."), *and* Dean Hachamovitch, *Windows Release Preview: The Sixth IE10 Platform Preview*, IEBLOG (May 31, 2012, 5:57 PM), http://blogs.msdn.com/b/ie/archive/2012/05/31/windows-release-preview-the-sixth-ie10-platform-preview.aspx ("In Windows 8, IE10 sends a 'Do Not Track' signal to Web sites by default. Consumers can change this default setting if they choose. This decision reflects our commitment to providing Windows customers an experience that is 'private by default' in an era when so much user data is collected online.").

[5] *See, e.g.*, *Tracking Preference Expression (DNT): W3C Editor's Draft 05 June 2013*, W3C, http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html (last visited June 21, 2013) [hereinafter *W3C TPE Draft*] ("This specification defines the technical mechanisms for expressing a tracking preference via the DNT request header field in HTTP, via an HTML DOM property readable by embedded scripts, and via properties accessible to various user agent plug-in or extension APIs.").

[6] *About W3C*, W3C, http://www.w3.org/Consortium/ (last visited Oct. 30, 2012) ("The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web Standards.").

[7] *W3C TPE Draft*, *supra* note 5.

[8] *See id.* ("[A] tracking preference expression is only transmitted when it reflects a deliberate choice by

programs—that simple tasks should be automated and integrated wherever possible to reduce transaction costs.[9]

¶4 At issue is whether Do-Not-Track will benefit the majority of consumers by providing a simple default, or whether it will only benefit those who find and set a privacy flag by hand.[10] The consequences of this decision are significant. Most consumers will benefit from Do-Not-Track if it is offered as a default feature of their browser. Most consumers will not benefit from Do-Not-Track if they must research, find, and set the flag by hand.[11] The debate over whether consumers can choose products that set Do-Not-Track by default is therefore critical to determining whether Do-Not-Track will work.[12]

¶5 Microsoft sparked the current debate by announcing that it would implement Do-Not-Track as a default feature in its next browser, Internet Explorer 10 (IE10). Privacy advocates lauded the decision.[13] The advertising industry did not.[14] Industry advocates

---

the user. . . . For example, a user might select a check-box in their user agent's configuration, install an extension or add-on that is specifically designed to add a tracking preference expression, or make a choice for privacy that then implicitly includes a tracking preference (e.g., 'Privacy settings: high').").

[9] *Cf.* EXPLOITING THE KNOWLEDGE ECONOMY: ISSUES, APPLICATIONS AND CASE STUDIES, PART 1 171 (Paul Cunningham & Miriam Cunningham eds., 2006) ("The Internet reduces transaction costs for business firms and provides consumers with more choices [and] more control . . . *in some cases*. By automating purchasing functions, companies can eliminate mistakes and costs . . . [and] the availability of information through automated systems also improves product flows . . . ." (emphasis added)); *see also* Margaret Jane Radin, *Reconsidering Boilerplate: Confronting Normative and Democratic Degradation*, 40 CAP. U. L. REV. 617, 652 (2012) ("Is it possible to use automation to enable consumers to get terms they would actually prefer? There are a few possibilities. . . . Online systems could . . . enable users to customize their own terms. . . . Filtering systems on personal computers would be market solutions because computer users would be free to use them or not use them . . . .").

[10] *See generally The Need for Privacy Protections: Is Industry Self-Regulation Adequate?: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (2012) [hereinafter *Self-Regulation Hearing*] (statement of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law, The Ohio State University), *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=aa018084-ceea-472c-af63-97d7f44fac80; *see also* Radin, *supra* note 9, at 654 ("Why are these possible automated systems not in use? . . . [P]erhaps it is believed that there is not a market for them."); *New Technologies and Innovations in the Mobile and Online Space, and the Implications for Public Policy: Hearing Before the Subcomm. of Intellectual Prop. and the Internet of the H. Comm. on the Judiciary*, 112th Cong. 72 (2012) [hereinafter Grimmelmann] (written testimony of James Grimmelmann), *available at* http://judiciary.house.gov/hearings/printers/112th/112-116_74641.PDF.

[11] *See* Kesan & Shah, *supra* note 4, at 601 ("If a person does not know about the possibility of changing an option or the ramifications of each choice, then a default setting is equivalent to a fixed setting.").

[12] *See* Grimmelmann, *supra* note 10 (written testimony of Professor James Grimmelmann) ("Users benefit from being able to delegate the choice to enable Do Not Track to Internet Explorer; it simplifies the option of choosing this form of privacy. Microsoft will succeed in the competitive browser market if and only if users consider this a valuable feature. But some other participants in the Do Not Track process, including representatives from Yahoo! and Google, have been pressing for the ability to disregard the Do Not Track request if it comes from a browser, like Internet Explorer, in which it is on by default. This attempt to sabotage the practical usability of Do Not Track would make it pointlessly harder for consumers to express their privacy preferences.").

[13] *See id.*

[14] *See* Julia Angwin, *Microsoft's "Do Not Track" Move Angers Advertising Industry*, WALL ST. J., May 31, 2012, http://blogs.wsj.com/digits/2012/05/31/microsofts-do-not-track-move-angers-advertising-industry/ ("Stu Ingis, general counsel of the [Digital Advertising Alliance], called Microsoft's move a 'unilateral' decision that 'raises a lot of concern.' He said that the industry supports 'consumer choice, not a choice made by one browser or technology vendor.'").

raised several inaccurate and irrelevant objections to default Do-Not-Track,[15] and threatened to ignore any DNT flag not intentionally set by the customer.[16]

¶6 Instead of bowing to pressure to remove default DNT, Microsoft set the Do-Not-Track flag by default as part of the express installation option.[17] Roy Fielding, an author of the TPE, responded by offering a patch for web servers that caused them to ignore all DNT flags set by Internet Explorer.[18] These developments may undermine the Do-Not-Track initiative.[19]

¶7 The debate over the TPE bespoke standard centers on the standard for online consent. Under the current language of the TPE draft, a default browser setting is not a valid expression of the user's will.[20] Although silence is not considered consent when consumers want to prevent tracking, silence is considered consent when consumers permit tracking. Consumers consent to tracking without doing a thing,[21] but cannot object to tracking even by buying and using browsers that offer automated enhanced privacy protection.[22]

¶8 The TPWG's bespoke standard binds consumers to corporate terms, and thus permits tracking, in the absence of consumer action. But consumers must take bespoke steps to bind corporations to consumer terms.[23] The TPE thus sets a precedent that is corrosive to future privacy features and to machine-mediated contracting online. It denies consumers the ability to manage their privacy preferences through automation software.

¶9 Privacy must be automated if it is to function.[24] If regulators and standard-setters endorse the view that an online action can only create a legal obligation if performed by

---

[15] *See id.*; Nehf, *supra* note 4, at 5 ("If consumers are aware . . . and deem privacy important, they are more likely to . . . avoid[] firms that might compromise their privacy interests and frequent[] the ones that are more likely to protect them."). *Compare* Hoofnagle et al., *supra* note 4, at 273–74 ("We empirically demonstrate that advertisers are making it impossible to avoid online tracking. Advertisers are so invested in the idea of a personalized web that they do not think consumers are competent to decide to reject it.").

[16] *See* Angwin, *supra* note 14.

[17] *See* Goodin, *supra* note 3 ("Critics of the Apache update contend Microsoft's Do Not Track implementation . . . is in compliance with the standard. A screen that is displayed when a user first uses the operating system offers two choices: Express settings and a more detailed Customized settings. The same screen explicitly states that choosing the Express option will turn on Do Not Track.").

[18] *See* Shankland, *supra* note 3.

[19] *See* Grimmelmann, *supra* note 10.

[20] *See W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.").

[21] *See* Hartzog, *supra* note 4, at 1648.

[22] *See, e.g.*, Sid Stamm, *Why We Won't Enable DNT by Default*, MOZILLA PRIVACY BLOG (Nov. 9, 2011), http://blog.mozilla.org/privacy/2011/11/09/dnt-cannot-be-default/ ("Mozilla's mission is to give users this choice and control over their browsing experience. We won't turn on Do Not Track by default because then it would be Mozilla making the choice, not the individual.").

[23] *Cf.* Hartzog, *supra* note 4, at 1642 ("It has become a truism that virtually no one reads standard-form online agreements. A recent study found that less than one in 1000 e-commerce website users read the terms of use. Even Supreme Court Chief Justice John Roberts has admitted he does not read the fine print on websites.").

[24] *See* EXPLOITING THE KNOWLEDGE ECONOMY, *supra* note 9, at 171 ("The Internet reduces transaction costs for business firms and provides consumers with more choices [and] more control . . . [and] the availability of information through automated systems . . . improves product flows . . . ."); Radin, *supra* note 9, at 651–54 (discussing the benefit of automated contracting for companies and that this benefit can be extended to consumers and tested in the market); Leon, *supra* note 2, at 589 (discussing the results of a

hand,[25] then future privacy features will either not be offered or not be effective. Requiring consumers to protect privacy by hand while permitting corporations to benefit from automation is like holding a race between a sprinter and a drag racer. No matter how much heart the sprinter shows, the race will be over before the sprinter gets off the starting block.[26]

¶10 This Article proceeds in three Parts. Part Two will provide a brief background on the Do-Not-Track debate and to the divergence of opinion over Do-Not-Track as default. Part Three will discuss a new theory of online privacy—that privacy must be fully automated to be at all effective. Part Four will provide specific responses to industry challenges and potential counterarguments to this Article's core assertions.

II. BACKGROUND

¶11 The first subpart discusses Do-Not-Track, its background, some details regarding its technical implementation, and some history of the debate over whether Do-Not-Track can be implemented as a default setting. The second and third subparts deal with the overall rise in automated software contracting and the legal literature of online contract and software automation.

A. Do-Not-Track

¶12 Do-Not-Track is a simple idea[27] that has been building for some time.[28] Its core concept is that consumers should be able to state that they do not agree to online tracking. Currently consumers are not able to do so, both because until recently there has been no technological way to communicate their preference and because courts and regulators have not yet enforced that preference even when communicated.[29] Before Do-Not-Track, a consumer's only option was to agree to online Terms of Service or End User License Agreements that permitted tracking, or to not use the service. The Do-Not-Track concept provides a technical method for delivering a legal message. Yet despite its simplicity, Do-Not-Track has created an extraordinary amount of debate.

---

study demonstrating the difficulty users have configuring privacy tools).

[25] *See, e.g.*, *W3C TPE Draft*, *supra* note 5.

[26] *See* Leon, *supra* note 2*; see also* Hoofnagle et al., *supra* note 4.

[27] *See* Joshua A.T. Fairfield, *"Do-Not-Track" as Contract*, 14 VAND. J. ENT. & TECH. L. 545, 545–46 (2012) ("When a consumer expresses her preference, in the very first exchange between the consumer and corporate computers, for the corporation not to track her information, the company is free to refuse the transaction if it does not wish to continue on the consumer's terms.").

[28] *See Self-Regulation Hearing*, *supra* note 10 (statement of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law, The Ohio State University).

[29] *See* Complaint at 10, Kim v. Space Pencil, Inc., No. CV-11-3796 (N.D. Cal. Aug. 1, 2011) (initiating a lawsuit against companies such as Spotify because of regenerative tracking cookies). *Cf.* Hoofnagle et al., *supra* note 4, at 292 ("Recently, Jonathan Mayer of Stanford University found that Google and other network advertisers . . . found a way to circumvent . . . cookie blocking. The method used by Google was particularly brazen—it opened a webpage invisible to the user and used a program to simulate the user clicking on it.").

1. The Do-Not-Track Flag

¶13 Consumer advocacy groups proposed Do-Not-Track to the Federal Trade Commission ("FTC") in 2007,[30] and researchers developed a prototype in 2009.[31] Do-Not-Track was loosely based on the FTC's successful Do-Not-Call list.[32] The FTC has on several occasions issued statements and staff reports encouraging some form of Do-Not-Track. The FTC has not yet, however, enforced Do-Not-Track flags against advertisers, preferring instead to wait on results from the self-regulatory process.[33] The vast majority of advertisers, therefore, continue to completely ignore consumers' clear statements that they do not consent to tracking.

¶14 The goal of Do-Not-Track was to provide a simple effective answer to the question of how consumers could express their desire not to be tracked.[34] The Do-Not-Track flag is set in the user's browser and is communicated to computers that the browser contacts via a message contained in the message header.[35] The DNT heading is contained in the information that the browser routinely exchanges with website servers. If the Do-Not-Track flag is enabled, then the user's browser tells everyone that the user does not consent to tracking.

¶15 Unlike the centralized federal Do-Not-Call list, no government agency maintains the proposed Do-Not-Track browser feature.[36] Do-Not-Call functions because telephone

---

[30] *See* 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 ("A coalition of privacy groups asked the government today to set up a mandatory do-not-track list for the Internet. The groups—which include the Consumer Federation of America, World Privacy Forum and several others—are worried that online advertising companies are collecting too much data about consumers' Web habits."); Ari Schwartz et al., *Consumer Rights and Protections in the Behavioral Advertising Sector*, CTR. FOR DEM. & TECH. 2, 4, https://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf (last visited June 22, 2013) ("[W]e urge the U.S. Federal Trade Commission (FTC) to take proactive steps to adequately protect consumers as online *behavioral tracking* and *targeting* become more ubiquitous. . . . [T]he FTC should: [c]reate a national Do Not Track List similar to the national Do Not Call List[.]"); Christopher Soghoian, *The History of the Do Not Track Header*, SLIGHT PARANOIA (Jan. 21, 2011), http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html ("In 2007, several public interest groups, including the World Privacy Forum, CDT and EFF, asked the FTC to create a Do Not Track List for online advertising.").

[31] *See* Soghoian, *supra* note 30 ("In July of 2009 . . . . [m]y friend and research collaborator Sid Stamm helped me to put together a prototype Firefox add-on that added two headers to outgoing HTTP requests: X-Behavioral-Ad-Opt-Out: 1 X-Do-Not-Track: 1.").

[32] *Id*. ("In a very savvy move, these groups named their scheme such that it instantly evoked the massively popular Do Not Call list. That is, even if the average person did not know how the Do Not Track list worked, it would sound like a good idea.").

[33] *See* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 3 (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf ("The Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online.").

[34] See donottrack.us for a list of academics, companies, and research groups associated with the effort to implement Do-Not-Track.

[35] Jonathan Mayer & Arvind Narayanan, *Do Not Track*, http://www.donottrack.us/ (last accessed Aug. 16, 2013) ("Do Not Track signals a user's opt-out preference with an HTTP header, a simple technology that is completely compatible with the existing web.").

[36] *See The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 112th Cong. (2012) (statement of Jon Leibowitz, Chairman, Federal Trade Commission), *available at* http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=4d001372-8bc0-

numbers are limited and static, and thus advertiser lists can be scrubbed against a government-maintained database. Since internet addresses change constantly, it would be difficult for a government entity to keep a list of IP addresses and require advertisers to not track them. And the protection would do users no good, since their IP addresses would change with the next session.

¶16 The Do-Not-Track flag is not a technological enforcement mechanism, and does not prevent companies from tracking against the consumer's wishes.[37] It merely states that the consumer does not consent to tracking. The bigger question is whether corporations should honor the Do-Not-Track flag when they see it. The Digital Advertising Alliance (DAA) had agreed in principle to honor browser-carried Do-Not-Track flags before it called that commitment into question over the issue of default Do-Not-Track.[38] It remains very doubtful whether the DAA or its members will follow through on that commitment, as discussed below.

¶17 A check-box in a browser is a standard method for communicating an enforceable legal preference. Clicking "I Agree" is the standard means of communicating online consent. Selecting "I Disagree" is no different. Yet nearly all online advertisers refuse in practice to respect users' clear and communicated preference not to be tracked. Notably, those advertisers do not simply deny a user access to a website or service unless that user permits tracking, as would be a company's unquestioned right. Instead, advertisers ignore the expressly stated contractual condition that has been unambiguously communicated to them and continue to track non-consenting users.

¶18 Do-Not-Track is a simple idea with broad support.[39] Advertisers have therefore attempted to undermine the standard by diluting it and threatening to withdraw support, rather than by directly opposing it. There are several lines of attack. The Digital Advertising Alliance claims that Do-Not-Track still permits them to collect information on consumers as long as they do not target consumers with ads.[40] This attempt to sidestep the purpose of Do-Not-Track has attracted some conversation. FTC representatives have suggested that the agency believes "Do-Not-Track" must mean "Do-Not-Collect."[41] Because the Do-Not-Collect issue has already gained traction, this article steps away

422d-a18b-308e7e4cd820 ("Do not track, of course, will be run by the industry, it won't be run like the government runs do-not-call.").

[37] *See* Hoofnagle et al., *supra* note 4, at 275–78.

[38] *See* Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism*, SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 22, 2012), https://www.aboutads.info/resource/download/DAA_Commitment.pdf ("Today the DAA announced that it will immediately begin work to add browser-based header signals to the set of tools by which consumers can express their preferences under the DAA Principles.").

[39] *See Need for Privacy Protections*, *supra* note 36 (statement of Jon Leibowitz, Chairman, Federal Trade Commission) ("[A]t this point, we are no longer asking whether do not track will exist but only how it will be implemented.").

[40] *See* Edward Wyatt & Tanzina Vega, *Conflict Over How Open 'Do Not Track' Talks Will Be*, N.Y. TIMES, Mar. 29, 2012, http://www.nytimes.com/2012/03/30/technology/debating-the-path-to-do-not-track.html ("The [Digital Advertising Alliance] . . . defines [Do Not Track] as forbidding the serving of targeted ads to individuals but not prohibiting the collection of data.").

[41] *See Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, FTC 53 (Mar. 2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf ("[A]n effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction.").

from the Do-Not-Collect debate to focus on the second, equally important, but less-theorized attack on the Do-Not-Track standard.

¶19 The second major assault on Do-Not-Track has attracted much less scrutiny. It has even garnered a moderate level of support among creators of the standard and developers with a reputation for pro-privacy software.[42] It is also the current position reflected in the W3C standard setting body's Tracking Preferences Expression (TPE) document. These entities seek a version of Do-Not-Track that would block Do-Not-Track as a default setting. Under the current TPE draft, companies would only support expressions of privacy protection that consumers set by hand.[43] Without timely and strong opposition, this bespoke standard for privacy preferences expression will become the rule. Not all stakeholders agree, however, and the debate is not yet over.

2. Default Do-Not-Track

¶20 There are deep divides in stakeholder views on Do-Not-Track as default.[44] In May 2012, Microsoft announced plans to ship Internet Explorer 10 (IE10) with the Do-Not-Track flag enabled by default.[45] Despite speculation that Microsoft would retreat from shipping IE10 with DNT enabled, Microsoft's Chief Privacy Officer Brendon Lynch reconfirmed in August that Microsoft's position on default Do-Not-Track was essentially unchanged.[46] Microsoft claimed in August 2012, contemporaneously with the manufacturing release of Windows 8, that consumer studies had convinced them that default Do-Not-Track was a popular choice.[47]

¶21 Microsoft crafted an interesting response to the W3C TPE demand that tracking preferences be set by hand.[48] Microsoft set the Do-Not-Track flag as part of the

---

[42] *See* Stamm, *supra* note 22 ("Do Not Track is intended to express an *individual's choice*, or preference, to not be tracked. It's important that the signal represents a choice made *by the person behind the keyboard* . . . .").

[43] *See W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. . . . We do not specify how tracking preference choices are offered to the user or how the preference is enabled . . . . [A] user might select a check-box . . . [or] install an extension or add-on . . . .").

[44] *See A Status Update on the Development of Voluntary Do-Not-Track Standards: Hearing Before S. Comm. On Commerce, Science, and Transportation*, 112th Cong. (2013), at 1:06:16, http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=1cf8fb1a-fb0b-4bf1-958b-1ea3c443a73c&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&YearDisplay=2013 (browser and advertising industry representatives disagreeing over the use of default blocking of cookies); Judith Aquino, *Privacy Advocate Jonathan Mayer Has Had It With 'Do Not Track'*, AD EXCHANGER (May 7, 2013, 3:31 PM), http://www.adexchanger.com/ad-exchange-news/privacy-advocate-jonathan-mayer-has-had-it-with-do-not-track/ ("Advertising companies have an incentive to convince users that . . . users should allow them to collect data. By setting those default settings to Do Not Track, we give interested parties the incentive to educate consumers about the impacts of [their] choices.").

[45] *See Self-Regulation Hearing*, *supra* note 10, at 23:50 (statement of Sen. Kelly Ayotte) ("As we all know Microsoft . . . announced Internet Explorer 10 will have its do-not-track component default set to opt-out of tracking.").

[46] *See* Brendon Lynch, *Do Not Track in the Windows 8 Setup Experience*, MICROSOFT ON THE ISSUES (Aug. 7, 2012, 9:00 AM), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/08/07/do-not-track-in-the-windows-8-set-up-experience.aspx.

[47] *Id.*

[48] *See id.*

installation process.[49] Users are informed that selecting express installation settings rather than custom installation will set the flag to Do-Not-Track.[50]

¶22 Note that IE10 is not the first browser to set Do-Not-Track by default. The TOR browser, for example, installs with a comprehensive list of privacy features already enabled.[51] The TOR browser is used precisely because it automates many features of privacy protection. Microsoft, however, has a far greater market reach. An IE10 rollout of default DNT would mean that most consumers would have a choice as to whether their browser sets Do-Not-Track by default or requires hand configuration. Thus, the pushback on default Do-Not-Track appears to be as much a response to Microsoft's market reach as to the existence of the pro-privacy feature.

¶23 The difference between a user setting a flag by hand in her browser and the same user agreeing to permit the express installation package in her browser to enable the same flag is conceptually interesting. The consumer, after all, does take an active step in deciding what version of Internet Explorer to install. That step might count as the active step that industry called for in the Tracking Preferences Expression. [52]

¶24 As attractive as this conciliatory approach is, however, it was not accepted by industry.[53] TPE author Roy Fielding promptly proposed a patch that would enable Apache web servers to ignore all Do-Not-Track flags sent by Internet Explorer.[54] The Digital Advertising Alliance also announced that it would not require members to respect DNT flags because of the question of default settings.[55] The debate over whether consumers may use default pro-privacy features is thus at the center of DNT implementation. If permitted, browsers could define themselves by adding default privacy features. Consumers would be able to make a choice for privacy by picking a browser that contains default, easy-to-use privacy features. Consumers who do not want privacy can use browsers that do not automatically configure privacy features. Consumers who do want privacy should be equally free to select products that incorporate automated privacy protection features, like the TOR browser, or, in the case of Do-Not-Track, IE10.

---

[49] *Id.*

[50] *Id.*

[51] *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 44 (2008) ("TOR is a type of 'mix network.' A mix network is structured in some ways like a peer-to-peer software trading network. . . . Through a series of clever cryptographic tricks . . . , none of the computers in the middle of the path can access the content of the communications nor discover the IP addresses of *both* the sending and receiving computers.").

[52] *Compare W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user."), *with* Nehf, *supra* note 4 ("If consumers are aware of their privacy concerns and deem privacy important, they are more likely to take steps to protect their own interests—for example, avoiding firms that might compromise their privacy interests and frequenting the ones that are more likely to protect them."), *and* Hoofnagle et al., *supra* note 4, at 295 ("[O]n a basic level, consumers' manifestations of *choice* should not be circumvented. . . . If advertisers wished to condition access to services on tracking, they could. But to do so, they would have to have some dialogue with the consumer, rather than resorting to sneaky technical methods to obscure the tracking.").

[53] *See Self-Regulation Hearing*, *supra* note 10, at 46:15 (statement of Berin Szoka, President, TechFreedom) ("Microsoft . . . decided in its new IE10 browser that it would set do-not-track headers by default. Default do-not-track-on doesn't empower users any more than would setting ad-blocking by default.").

[54] *See* Shankland, *supra* note 3.

[55] *See* Angwin, *supra* note 14.

3. The TPWG's Tracking Preferences Expression Standard

¶25 The core of the advertising industry's resistance to default Do-Not-Track relied on language from the TPWG's TPE standard. That standard permits advertisers to ignore any DNT flag that the advertiser suspects to have been automatically set by a browser. This would require privacy-seeking consumers to set the flag by hand. This subpart examines the language of the TPE in more detail. As the TPE is not a finished document, this Article limits its analysis to language available at the time the Article was drafted. Readers may wish to consult further drafts of the TPE as the debate moves forward.

¶26 The TPE's adoption of a bespoke standard for privacy flags was ostensibly to protect consumer choice against third parties who would seek to make consumers' choices for them.[56]

> The goal of this protocol is to allow a user to express their personal preference regarding tracking to each server and web application that they communicate with via HTTP, thereby allowing each service to either adjust their behavior to meet the user's expectations or reach a separate agreement with the user to satisfy all parties.
>
> Key to that notion of expression is that the signal sent MUST reflect the user's preference, not the choice of some vendor, institution, site, or any network-imposed mechanism outside the user's control . . . . The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.[57]

¶27 Yet the TPWG itself is an "institution . . . outside the user's control"[58] that seeks to make a choice for the user that does not reflect a "deliberate choice by the user."[59] This is because "in the absence of user choice, there is no tracking preference expressed."[60] To the TPWG, this means that tracking is permitted when consumers have not given consent. The TPWG's current structure for the Tracking Preferences Expression makes consumers' choices for them, while denying consumers the right to select any other trusted source, such as a browser with a reputation for privacy, to provide a comprehensive suite of privacy enhancements.

¶28 A consumer's choice to use a pro-privacy browser is a better indication of consent than is silence—which is what the TPE uses as adequate grounds to justify tracking. A pro-privacy browser is a better reflection of the desires of its users than is the TPE.

---

[56] *See* W3C *TPE Draft*, *supra* note 5.

[57] *Id*.

[58] *Id.*; *see also Participation*, W3C, http://www.w3.org/participate/ (last accessed Sept. 10, 2012) ("Participation in W3C Working Groups . . . is open to W3C Members and other invited parties. W3C groups work with the public through specification reviews as well as contributions of use cases, tests, and implementation feedback."). Members of the public may join, but only as experts. *See Instructions for Non-Members (Invited Experts)*, W3C, http://www.w3.org/2004/08/invexp.html (last accessed Sept. 10, 2012). General members of the public have minimal interaction, let alone control, with W3C working groups, specifically the Tracking Protection Working Group.

[59] *W3C TPE Draft*, *supra* note 5.

[60] *Id.*

Consumers who desire privacy will rationally choose those products that not only provide the most privacy features, but also those which permit them to be used at the lowest cost. It is not reasonable to claim that that rational choice does not reflect the desire of the consumer.

¶29 Assume that neither "please-track-me" nor "do-not-track" represents the wishes of all consumers. Some prefer one, and others prefer the other. The real question is which rule is best to set as a default, and how to reduce the transaction costs of the switching group.[61] This shows the problems with the TPWG's analysis. It sets the default rule (tracking) to one that very few people want and raises the cost of switching away from that default as high as possible. But in the Coasean sense, the best answer is not only to permit each party to choose what they want,[62] but also to reduce transaction costs as much as possible.[63]

¶30 Most Americans oppose online tracking.[64] There is a reasonable case to be made that the default rule ought to be set to the majoritarian default—Do-Not-Track.[65] This minimizes the number of people who need to incur transaction costs in order to satisfy preferences. Yet no matter what the default, surely it would be better to permit parties who do not agree with the majority to satisfy their privacy preferences with the lowest possible transaction costs. The TPWG's standard would force consumers to set their privacy preferences by hand when those preferences could be set automatically through the consumer's choice of browser. The TPE standard raises transaction costs regardless of the consumer's preference.[66]

---

[61] *See generally Self-Regulation Hearing*, *supra* note 10. *See also* Kesan & Shah, *supra* note 4, at 601 ("If a person does not know about the possibility of changing an option or the ramifications of each choice, then a default setting is equivalent to a fixed setting."). *But see* Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 *SCRIPTED* 155, 156 (2010), *available at* http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.pdf ("Where discussion diverges into heated debate is in the use of rhetorical terms that simplify the discussion into one of black and whites, when really there are a range of practices and solutions that deserve inspection.").

[62] R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 19 (1960) ("Even when it is possible to change the legal delimitation of rights through market transactions, it is obviously desirable to reduce the need for such transactions and thus reduce the employment of resources in carrying them out.").

[63] *Id.* at 8 ("[T]he ultimate result (which maximises the value of production) is independent of the legal position if the pricing system is assumed to work without cost.").

[64] *See* KRISTEN PURCELL, JOANNA BRENNER, & LEE RAINIE, PEW INTERNET PROJECT, SEARCH ENGINE USE 2012 39 (Mar. 9, 2012), *available at* http://pewinternet.org/~/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf ("68% [of Americans polled stated] I'm NOT OKAY with targeted advertising because I don't like having my online behavior tracked and analyzed."); MARY HODDER ET AL., CUSTOMER COMMONS, LYING AND HIDING IN THE NAME OF PRIVACY (2013), http://customercommons.org/wp-content/uploads/2013/05/CCResearchSurvey1Paper_Final.pdf ("[P]eople limit, refuse to give or obfuscate personal information in an attempt to create a measure of privacy online."); Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 30, 2009, http://www.nytimes.com/2009/09/30/business/media/30adco.html ("About two-thirds of Americans object to online tracking by advertisers—and that number rises once they learn the different ways marketers are following their online movements . . . .").

[65] *See, e.g.*, PURCELL, BRENNER, & RAINIE, *supra* note 64; HODDER ET AL., *supra* note 64; Hoofnagle et al., *supra* note 4, at 295 ("[O]n a basic level, consumers' manifestations of choice should not be circumvented. . . . If advertisers wished to condition access to services on tracking, they could. But to do so, they would have to have some dialogue with the consumer, rather than resorting to sneaky technical methods to obscure the tracking.").

[66] *Cf.* Hoofnagle et al., *supra* note 4, at 273 ("We empirically demonstrate that advertisers are making it impossible to avoid online tracking. Advertisers are so invested in the idea of a personalized web that they do not think consumers are competent to decide to reject it."). *But see* Stuart Ingis, *Fears of Online*

¶31 The problem is inherent in the implementation of the DNT flag. Do-Not-Track is, logically speaking, a binary flag. The value of Do-Not-Track is equal to zero or one. The switch is either "on" or "off".[67] Yet there is a third state in the protocol, "unset," and the unset state must be provided by every software agent designer. Given that DNT:1 means that tracking is forbidden, and DNT:0 means that tracking is permitted, the unset term serves only as a gap-filler, a placeholder, a state from which every consumer must take action at non-zero cost, in order to reach his or her true preference.[68]

¶32 The no-default rule stops the consumer from escaping the cost of having to set the flag from "unset" to either "track" or "do-not-track" by selecting a browser. The TPE working document states:

> A user agent **must not** send a tracking preference expression if a tracking preference is not enabled. This means that no expression is sent for each of the following cases:
>
> - the user agent does not implement this protocol;
> - the user has not yet made a choice for a specific preference; or,
> - the user has chosen not to transmit a preference.[69]

¶33 In so doing, the TPWG has set an undesirable standard both in technology and in law. It sets the worst rule as the default and raises the costs of switching away from that rule. The rule therefore increases costs for most users.

¶34 The rule is also inconsistent in how it treats consumers and advertisers. Under the TPE standard, software defaults create no enforceable rights in the hands of a consumer.[70] Yet software defaults create perfectly enforceable rights in the hands of advertisers.[71] The result of the TPE's bespoke requirement for preference expression is that a company is free to ignore the Do-Not-Track flag if it suspects that the flag was set automatically by software rather than manually by a consumer.

¶35 The question is therefore not merely one of privacy and consumers' rights. The deeper issue at play is whether consumers will be permitted to benefit from the massive rise in software agent contracting.[72] If the TPWG's no-default rule stands, it will be a

---

Tracking Are Baseless, US NEWS, Aug. 20, 2012, http://www.usnews.com/opinion/articles/2012/08/20/fears-of-online-tracking-are-baseless ("[T]here have been efforts to shift from an open and seamless Internet to one where collection is not permissible unless a consumer opts in. This approach would harm the online experience and is unnecessary because robust industry self-regulation is already giving consumers transparency and choice over online data collection.").

[67] *See Do Not Track Us*, *supra* note 4 ("Do Not Track provides users with a single, simple, persistent choice to opt out of third-party web tracking.").

[68] *See* Tom Lowenthal, *Deeper Discussion of our Decision on DNT Defaults*, MOZILLA PRIVACY BLOG (Nov. 15, 2011), http://blog.mozilla.org/privacy/2011/11/15/deeper-discussion-of-our-decision-on-dnt-defaults/ ("DNT:0 means 'I consent to being tracked.' DNT:1 means 'I object to being tracked.'").

[69] *See W3C TPE Draft*, *supra* note 5.

[70] *See id.* ("[A] tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed. . . . If the user's choice is DNT: 1 or DNT: 0, the tracking preference is *enabled* . . . .").

[71] *See id.* ("If the user's choice is DNT:1 or DNT:0, the tracking preference is *enabled* . . . .") .

[72] *See* Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303, 3056 n.3 (2008) ("[T]he digital environment can *potentially* offer a very different contractual setting, providing consumers with an 'electronic butler' that will automatically signal . . . preferences to . . . vendors." (emphasis added)); *see also* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 227–28 (2008) ("[W]e

serious blow to consumers well beyond the Do-Not-Contract context. If consumers are required to contract by hand online, they will be so swamped with transaction costs that they will not be able to adequately protect their privacy interests.[73]

¶36 The TPE bespoke standard privileges feature choice over product choice. Under the standard, consumers must configure features. They may not pick browsers that have a systematic approach to integrating and automating privacy protections.[74] A consumer can only choose to increase her privacy protection through the roundabout method of choosing a browser that does not protect her privacy, and then modifying and configuring it so that it does.

¶37 Consider an analogy. Suppose a consumer wanted to purchase a fast car. Under Regulatory Climate A, that consumer could choose a car built by a manufacturer with a reputation for speed. The speed might be reflected in a range of features, from engine design to aerodynamics. Under Regulatory Climate B, the consumer is forbidden to select a car with an overall reputation for speed. She must rather research each feature, and in fact do some of the bodywork herself. The difference between Regulatory Climates A and B is whether the consumer may make a choice at the product level or the feature level. In both cases the consumer makes a choice. The difference is in the cost of the choice to the consumer.

¶38 Just as consumers should be able to choose cars with a combined feature set that makes them fast, consumers should be able to choose browsers with a combined feature set that makes them private. Further, to say that a consumer who picks an overall fast car does not have a discernible preference for speed is incorrect. The claim that consumers who use integrated-feature-set browsers do not have a discernible preference for privacy is equally wrong.[75]

---

need ways for people to signal whether they would like to remain associated with the data they place on the Web, and to be consulted about unusual uses. . . . [W]e will face the question of when people ought to be informed when their online behaviors are used for ulterior purposes—including beneficial ones."); LAWRENCE LESSIG, CODE: VERSION 2.0 228–29 (2006) http://codev2.cc/download+remix/Lessig-Codev2.pdf ("[A] privacy property right would create strong incentives in those who want to use that property to secure the appropriate consent. . . . But without that consent, the user of the privacy property would be a privacy pirate. Indeed, many of the same tools that could protect copyright in this sense could also be used to protect privacy."); CREATIVE COMMONS, http://creativecommons.org/about (last visited Sept. 5, 2012) ("[The creative commons system] give[s] everyone from *individual* creators to large companies . . . a *simple, standardized* way to keep their copyright while allowing certain uses of their work . . . ." (emphasis added)). *But see* 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, 284–85 (2012) ("Practical progress advancing user privacy will be better served if policymakers and industry focus their debate on the desirable balance between efficiency and individual rights, and on whether businesses implement tracking mechanisms fairly and responsibly."). For further discussion, see *infra* Section II(B), Software Agents and Automation.

[73] *Cf.* Hartzog, *supra* note 4; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. OF L. & POL'Y FOR THE INFO. SOC'Y 543, 546 (2008); Jared S. Livingston, *Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting*, 21 ALB. L.J. SCI. & TECH. 591, 626 (2011) ("[F]irms have the incentives and opportunities to impose additional costs on users to keep them from investing in research about the agreement (footnote omitted) . . . . So not only do consumers already not care to read their agreements, but firms can also make it worse, both of which make exploitation more likely.").

[74] *See W3C TPE Draft*, *supra* note 5.

[75] *See* discussion *infra* accompanying note 80*; see also* Grimmelmann, *supra* note 10 ("Users benefit from being able to delegate the choice to enable Do Not Track to Internet Explorer; it simplifies the option of choosing this form of privacy. Microsoft will succeed in the competitive browser market if and only if users consider this a valuable feature. But some other participants in the Do Not Track process, including

¶39 The TPE bespoke standard bans product-level choice with one exception. The exception proves the problem. The TPE draft states consumers may only exercise product-level consent by choosing a browser whose name includes the privacy preference.[76] The exception only covers browsers whose very name includes the word "privacy" or the like in the name of the browser itself. This excludes any mainstream browser from developing automatic and integrated default pro-privacy features.[77] The Draft states:

> A user agent MUST have a default tracking preference of unset (not enabled) unless a specific tracking preference is implied by the decision to use that agent. For example, use of a general-purpose browser would not imply a tracking preference when invoked normally as "SuperFred", but might imply a preference if invoked as "SuperDoNotTrack" or "UltraPrivacyFred". Likewise, a user agent extension or add-on MUST NOT alter the tracking preference unless the act of installing and enabling that extension or add-on is an explicit choice by the user for that tracking preference.[78]

¶40 This makes as much sense as requiring Ferrari to include "fast" in the names of their cars. The most important expression of choice is the consumer's choice of which product to use. The requirement that the selection must be of a browser that has some designation of privacy preference in the name guts the exception.

¶41 Brand loyalty must be built on a range of features. A user might very well choose one browser over another because of additional privacy features,[79] even though those are not the only features for which the browser is known. Privacy features, like other features, play into the consumers' choice of which browser to use.[80] This is no less a demonstration of user intent than is hand-configuring privacy features.

¶42 The "name" standard for browsers stops new pro-privacy brands from building name recognition. Consider the TOR Browser. It is certainly the browser that the TPE intended to protect when exempting special browsers from the requirement that privacy cannot be the default in browsers.[81] Yet there is nothing in the TOR name that indicates that the TOR Browser is a byword in privacy circles. One must first know that TOR

---

representatives from Yahoo! and Google, have been pressing for the ability to disregard the Do Not Track request if it comes from a browser, like Internet Explorer, in which it is on by default. This attempt to sabotage the practical usability of Do Not Track would make it pointlessly harder for consumers to express their privacy preferences." (footnote omitted)).

[76] *See W3C TPE Draft*, *supra* note 5.

[77] *See* Grimmelmann, *supra* note 10.

[78] *See W3C TPE Draft*, *supra* note 5.

[79] *See* Hachamovitch, *supra* note 4 ("[W]e think . . . consumers will favor products designed with their privacy in mind over products that are designed primarily to gather their data.").

[80] *See* Nehf, *supra* note 4 ("If consumers are aware of their privacy concerns and deem privacy important, they are more likely to take steps to protect their own interests—for example, avoiding firms that might compromise their privacy interests and frequenting the ones that are more likely to protect them."); *see also* Hachamovitch, *supra* note 4; Scott Cleland, *Why We Need A 'Do-Not-Track' Bill*, WASH. POST, May 10, 2011, http://live.washingtonpost.com/why-you-cant-trust-google-scott-cleland-0510.html ("People deserve the right to vote for themselves if they want to be tracked . . . . [R]ight now people have no real choice because the technology is way ahead of what people want and the state of the law.").

[81] *See W3C TPE Draft*, *supra* note 5 ("[U]se of a general-purpose browser would not imply a tracking preference when invoked normally as 'SuperFred', but might imply a preference if invoked as 'SuperDoNotTrack' or 'UltraPrivacyFred'.").

stands for "the onion router," and what that means in turn, to understand that anyone who uses the TOR browser has clearly indicated by their choice to do so that they do not wish to be tracked.[82] The most famous default privacy browser would, by the TPE's name standard, be prohibited from building the very reputation for privacy it currently enjoys.

¶43 Conversely, the UltraPrivacyFred standard prohibits mainstream browsers from retaining their customer goodwill while adding automated privacy features.[83] Internet Explorer can never meet the "name" standard. In order to gain a reputation for privacy protection, it would have to be named InternetPrivacyExplorer or something similar, thus denying it brand recognition and customer goodwill. Similarly, mainstream browsers would have a problem building an actual reputation for privacy, since in order to do so they would have to set the DNT flag by default, which would mean that the DNT flag would be ignored, thus denying their users privacy protections. This in turn would erode the reputation for privacy that the brand might attempt to build.

¶44 Consumer choice is most often expressed at the product level, not at the feature level. Building a brand based on privacy requires that companies be free to add privacy features without retaliation from industry groups. Browser creators should not have to fork their products into separate, privacy-themed browsers. The bespoke standard, which requires feature-level choice rather than product-level choice, therefore significantly inhibits competition in the privacy market.[84]

4. The Problems of Default and Compliance

¶45 It is also worth discussing how default and compliance work within the TPE framework.[85] The question of default matters because in order to enforce a rule against defaults, one must have an idea of what a default is. The question of compliance matters because even if IE10's installation implementation runs afoul of the "no default" rule—and this is by no means certain[86]—there remains the issue of how websites may respond while continuing to represent that they are compliant with the DNT standard.

---

[82] *See Tor: Overview*, TORPROJECT, https://www.torproject.org/about/overview.html.en (last accessed Apr. 2, 2013) ("Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers.").

[83] *Cf. W3C TPE Draft*, *supra* note 5.

[84] *See* Nehf, *supra* note 4 ("If consumers are aware of their privacy concerns and deem privacy important, they are more likely to take steps to protect their own interests—for example, avoiding firms that might compromise their privacy interests and frequenting the ones that are *more likely* to protect them." (emphasis added)*; see also* PURCELL, BRENNER, & RAINIE, *supra* note 64, at 3 ("Just 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website. Among this group, one common strategy people use to limit personal data collection is to delete their web history: 81% of those who know ways to manage the capture of their data do this. Some 75% of this group uses the privacy settings of websites to control what's captured about them. And 65% change their browser settings to limit the information that is collected.").

[85] The Author is indebted to Professor James Grimmelmann for raising and discussing the points in this subpart in comments on a draft of this paper.

[86] *See* Jonathan Mayer, Comment to *Bug 53845 - Remove DNT Settings from httpd.conf*, APACHE SOFTWARE FOUND. (Sept. 9, 2012, 4:02 AM), https://issues.apache.org/bugzilla/show_bug.cgi?id=53845 ("The group has *not*, however, decided . . . [a]n installation/first-run option, like shipping Internet Explorer 10, is noncompliant. The draft text, in fact, notes this is an acceptable implementation . . . .").

¶46 The problem of what constitutes a compliant response to a default DNT flag can be broken down into two broad parts. The first asks what a default setting is.[87] The second asks what it means when an advertiser states that she is compliant with the DNT standard. This subpart will address each in turn.

¶47 *a) Undertheorization of Default.*—What constitutes a default setting is unclear. In an email to the TPWG, professor and author James Grimmelmann sets out the basic problem. The TPE standard tries to require deliberate choice and avoid ambiguity while prohibiting requiring any specific form of user interface.[88] But these three factors are not independent of one another. Unambiguity as to user choice requires that the user interface record and transmit the actions of the user in reaching that choice, as well as any actions that the browser takes in setting up that choice.[89] To know what the user has chosen, one must know both what the user does and how the browser operates.[90]

¶48 Assume, for the sake of argument, that when Microsoft asks customers whether they want to do an express install (which enables DNT) or a custom install,[91] it still presents too much of a default setting and not enough of a deliberate choice. The argument is incorrect[92] but plausible. This tells us nothing about whether a browser could frame the choice in other ways.

¶49 The TPE itself notes that the choice of tracking preference might be presented in a range of ways.[93] The TPE notes that a prompt at first use or a prompt after an update are acceptable.[94] The distance between a prompt at first use and the prompt at installation offered by IE10 is not very large, if it exists at all.[95] Nor is it clear how far along the short distance between a prompt at installation and a prompt at first use a browser must

---

[87] *See* E-mail from James Grimmelmann, Professor of Law, New York Law School, to Roy T. Fielding (Sept. 12, 2012, 7:35 PM), *available at* http://lists.w3.org/Archives/Public/public-tracking/2012Sep/0167.html.

[88] *See id.*

[89] *See id*.

[90] *See id.*

[91] *See* Goodin, *supra* note 3 ("Critics of the Apache update contend Microsoft's Do Not Track implementation . . . is in compliance with the standard. A screen that is displayed when a user first uses the operating system offers two choices: Express settings and a more detailed Customized settings. The same screen explicitly states that choosing the Express option will turn on Do Not Track.").

[92] *See W3C TPE Draft*, *supra* note 5 ("The user-agent might ask the user for their preference during startup, perhaps on first use or after an update adds the tracking protection feature. Likewise, a user might install or configure a proxy to add the expression to their own outgoing requests."); Goodin, *supra* note 3.

[93] *See W3C TPE Draft*, *supra* note 5 ("We do not specify how tracking preference choices are offered to the user or how the preference is enabled . . . . For example, a user might select a check-box in their user agent's configuration, install an extension or add-on that is specifically designed to add a tracking preference expression, or make a choice for privacy that then implicitly includes a tracking preference (e.g., 'Privacy settings: high').").

[94] *See id.* ("The user-agent might ask the user for their preference during startup, perhaps on first use or after an update adds the tracking protection feature. Likewise, a user might install or configure a proxy to add the expression to their own outgoing requests.").

[95] To clarify, when you install a browser such as IE10, the install process includes clicking to download the browser from an installation of Windows or directly from a website. An install wizard walks a user through options, such as a standard or custom install. Within seconds the browser can install and appear on a user's desktop. A quick click opens the browser. Two prompts appear: one at the time of install and one at the time of first use to adjust settings. The gap between these prompts can easily be shorter than 60 seconds.

travel in order to trigger the "no default" rule. Browsers have countless ways to influence consumers' decisions by framing, prompting, packaging, or reminding.[96]

¶50 For example, it is not at all clear from the TPE standard how strongly or often a browser can present the choice. The TPE explicitly references a choice presented regularly at startup,[97] which is likely to have a strong effect. It is possible to construct a browser presentation of choice in such a way that it has the same effect as a default. A browser might employ regular reminders like some anti-malware programs do, in this case reminding the user that she is browsing with a flag unset and offering her a simple button to click to set the flag. If the reminders are set one way—that is, if the user is prompted to set the flag but not unset the flag—there is no question that it will change outcomes.[98] Even though some form of regular reminder or prompt is contemplated by the TPE, there is no doubt that browser prompting of this sort would come under heavy fire by advertisers as violating the "no default" rule.

¶51 The point is not just that the rule is unclear. Any rule can be criticized by pointing out close cases and outliers. The problem is that the rule, according to its own terms, requires unambiguity. The compliance of the advertiser can be measured only if user choice is unambiguous. However, user choice must be ambiguous if the TPE does not dictate how the User Interface presents, records and transmits the record of the consumer's choice.[99] The standard vanishes if the advertiser has the power to judge ambiguities itself. The risk is that the determination of whether an advertiser must comply with a Do-Not-Track flag will be resolved entirely based on the self-interested guesses of advertisers, as the next section details.

¶52 *b) Tracking Compliance*.—Even if an incoming set DNT flag is determined to be an impermissible default setting, there is the question of how a website can respond while remaining DNT-compliant.[100] This matters from a regulatory standpoint. A website's statement that it is DNT-compliant is precisely the sort of consumer-facing promise that will trigger the FTC's ability to enforce.[101] Compliance is defined in another W3C work in progress, termed Tracking Compliance and Scope (TCS).[102] The TCS interacts with the TPE in that the latter specifies how a preference may be indicated, while the former discusses how user agents and tracking entities must comply. In discussing compliance,

---

[96] *See* Kesan & Shah, *supra* note 4, at 591–92 ("The malleability of software means that developers can add, remove, or change default settings. A typical program has tens (and up to hundreds) of defaults that are set by the developer. . . . These defaults often come in the form of alert or confirmation boxes.").

[97] *See W3C TPE Draft*, *supra* note 5 ("We do not specify how tracking preference choices are offered to the user or how the preference is enabled . . . . The user-agent might ask the user for their preference during startup . . . .").

[98] *See* Kesan & Shah, *supra* note 4.

[99] *See* E-mail from James Grimmelmann, *supra* note 87.

[100] Thanks to James Grimmelmann for comments suggesting this framework and the issues in this sub-part.

[101] *See Making Sure Companies Keep Their Privacy Promises to Consumers*, FTC, http://ftc.gov/opa/reporter/privacy/privacypromises.shtml (last modified Jan. 28, 2013) ("When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. As of May 1, 2011, the FTC has brought 32 legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information.").

[102] *See Tracking Compliance and Scope: W3C Working Draft 30 October 2013*, W3C, http://www.w3.org/TR/2012/WD-tracking-compliance-20121002 (last visited July 13, 2013).

therefore, it is useful not only to discuss how a browser must comply with the standard, but also to discuss how a tracking server must comply when it receives a flag.

¶53 When a server encounters a DNT flag that might violate the "no default" rule, what may a server do? This is as yet undefined, and there are at least four options.[103] First, the entire browser might be considered noncompliant because it sets some flags automatically. It might then follow that the server would not be obliged to respect any flag the browser sends. Second, the browser might be considered to be sometimes compliant, since some flags are set automatically, but some are set by hand. As a result, the server might be permitted to ignore all flags set by the server because it cannot determine which flags are legitimate and which are not. Third, the entire browser might be considered non-compliant, but because the DNT flag has been sent, the server might be required to comply with the flag. And fourth, the browser might be considered sometimes compliant, but the server might be required to comply with some default-set DNT flags in order to meet its obligation to honor all compliant flags. The first and second positions represent the advertiser position, and penalize all users of a given browser if any user of that browser benefits from a default setting. The third and fourth positions represent the consumer advocate position, and do not permit the advertiser to ignore all flags by a browser merely because some flags might be improperly set.

¶54 It helps to measure these positions by their impact on the overall standard. The industry position destroys the standard. As in the above subpart, there are serious disagreements about what forms of user interface violate the "no default" rule. If the result of this unavoidable ambiguity is that a tracking server may ignore all flags—including those set manually—the standard will cease to have any effect. If advertisers can claim doubt as to the compliance of any subset of how the DNT option is presented, they could refuse to respect all flags from that browser, while still claiming that they are in compliance with Do-Not-Track as an overall standard.

¶55 The consumer advocate position does not destroy the standard. It resolves inevitable ambiguities regarding user interfaces in favor of respecting flags. The counterargument is that it hurts companies by limiting their ability to track consumers. In deciding which approach is best, it is useful to note that both of these positions get some cases wrong. The advertiser position incorrectly handles all flags actually set by users who do not want to be tracked. The consumer position incorrectly handles flags set by people who do wish to be tracked, but who have not set their tracking preference to '0'. The advertiser position invades privacy. The consumer position creates inconvenience.

¶56 The errors differ quantitatively as well as qualitatively. The advertiser position will categorize more cases incorrectly than will the consumer position, because the majority of consumers do not want to be tracked.[104] If some few consumers do wish to be tracked, they can opt in by setting DNT to '0' for the same costs of unchecking a box that the standard now imposes on the majority of consumers.

¶57 Resolving the necessary ambiguities created by different user interfaces in favor of permitting tracking will not merely impact default DNT. It will remove the obligation to respect DNT altogether, whether the flag is bespoke or automatically set. Resolving

[103] Thanks to James Grimmelmann for this framework, suggested in comments on earlier drafts of this article.

[104] *See* PURCELL, BRENNER, & RAINIE, *supra* note 64; HODDER ET AL., *supra* note 64.

ambiguity in favor of respecting DNT removes the moral hazard of companies deciding for themselves whether they may track, and results in fewer and less damaging errors.

B. Software Agents and Automation

¶58 Do-Not-Track is merely the crest of an underlying wave of automated contracting through software agents.[105] Software agent contracting has been a mainstay of business-to-business contracting for a long time.[106] There is, however, a problem with the current system. Consumers have little access to automated contracting tools.[107] Consider, for example, how long it has taken to provide consumers with a simple check-box that indicates whether or not they agree to being tracked. E-commercial systems are designed very carefully to prevent consumers from expressing any contractual preference other than assent to the corporation's End User Licensing Agreement (EULA) or Terms of Service (TOS).[108]

¶59 Software agents have been around as long as computers. Computers automate simple, repetitive tasks.[109] Human/computer interaction works best when humans use high-level judgment and computers automatically handle the details. Automation and computing technology are fundamentally inseparable.[110] Consequently, it is odd to insist that a human perform a simple and easily automatable task, like setting a Do-Not-Track flag, by hand.

¶60 There is a better solution. What consumers or companies want to automate, they should be able to automate.[111] Companies should not be free to selectively require their

---

[105] *See* Eric J. Feigin, Note, *Architecture of Consent: Internet Protocols and Their Legal Implications*, 56 STAN. L. REV. 901, 902 (2004) ("Higher-level protocols . . . involve exchanges that should be considered express consent: the formation of a legally binding contract.")*; see generally* Séverine Dusollier, *The Master's Tools v. The Master's House: Creative Commons v. Copyright*, 29 COLUM. J.L. & ARTS 271 (2006); Amelia H. Boss, *Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment*, 13 NW. J. INT'L L. & BUS. 31 (1993).

[106] *See, e.g.*, KEE-HUNG LAI & T.C.E. CHENG, JUST-IN-TIME LOGISTICS 16–17 (2009) (describing the emergence of Just-in-Time (JIT) management approach in the services sector during the 1990s, with particular emphasis on Wal-Mart's model).

[107] *See* Becher & Zarsky, *supra* note 72, 308–14; *see also* Hartzog, *supra* note 4, at 1636; Charles L. Knapp, *Opting Out or Copping Out? An Argument for Strict Scrutiny of Individual Contracts*, 40 LOY. L.A. L. REV. 95, 101–04 (2006) (discussing how dominance of the drafter has become typical in contract law). Consumers lack access to automated contracting tools, let alone a seat at the contracting table.

[108] For example, when you shop on Amazon.com, you are bound by multiple pages of terms in the Amazon Terms of Service. The only contract terms you may send to Amazon are what you want, how fast, and how many.

[109] *See, e.g.*, LESSIG, *supra* note 72, at 209 ("The great flaw to the design of *1984* was in imagining just how it was that behavior was being monitored. These were no computers in the story. The monitoring was done by gaggles of guards watching banks of televisions. . . . [T]here was no single guard who had a complete picture . . . . [T]hat 'imperfection' can now be eliminated. We can monitor everything and search the product of that monitoring. Even Orwell couldn't imagine that.").

[110] *See, e.g.*, *id.* at 22 ("[E]fficiency is made possible by technology, which permits searches that before would have been far too burdensome and invasive.").

[111] *See* EXPLOITING THE KNOWLEDGE ECONOMY, *supra* note 9 ("The Internet reduces transaction costs for business firms and provides consumers with more choices [and] more control . . . . [T]he availability of information through automated systems also improves product flows . . . .")*; see also* Radin, *supra* note 9, at 651–54 (discussing the benefit of automated contracting for companies and that this benefit can be extended to consumers and tested in the market); Hoofnagle et al., *supra* note 4, at 295 ("[O]n a basic level, consumers' manifestations of choice should not be circumvented. . . . If advertisers wished to condition access to services on tracking, they could. But to do so, they would have to have some dialogue with the

customers to engage in bespoke contracting activity at a given point within an otherwise completely automated process. If legal rules were to dictate otherwise, they would place a heavy hand on the scales of the market.[112] An automation ban prohibitively raises transaction costs on whichever party is barred from the use of automated tools and features. Corporations that can deprive customers of privacy using automated tools will always beat consumers who have to protect their rights by hand.[113]

C. The Legal Underpinnings of Do-Not-Track

¶61 Law is deeply involved in the Do-Not-Track debate. If stakeholders can agree on the implementation of a Do-Not-Track TPE standard,[114] the FTC may adopt that standard and give it the effect of law,[115] whether the FTC operates under its Section 5 authority,[116] or under separate authority from future legislation.

¶62 Legal theory, and especially the theory of contractual consent, is also central to the Do-Not-Track debate. That debate is extremely interesting in that it is a debate about a technical standard largely conducted in legal language. The central debate over Do-Not-Track is whether a consumer must set the Do-Not-Track flag by hand in order for it to

---

consumer, rather than resorting to sneaky technical methods to obscure the tracking.").

[112] *Compare* Angwin, *supra* note14, *and W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a *deliberate choice by the user*. In the absence of user choice, there is no tracking preference expressed." (emphasis added)), *with* Nehf, *supra* note 4, *and* Hachamovitch, *supra* note 4 ("[W]e think . . . consumers will favor products designed with their privacy in mind over products that are designed primarily to gather their data.").

[113] *See* Nehf, *supra* note 4 ("Without prohibitively high transaction costs or impediments to understanding the varying privacy practices of competing firms, informed consumer choices should produce more efficient privacy practices online."); *see also* PURCELL, BRENNER, & RAINIE, *supra* note 64, at 3 ("Just 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website."); Hoofnagle et al., *supra* note 4, at 273–74 ("We empirically demonstrate that advertisers are making it impossible to avoid online tracking. Advertisers are so invested in the idea of a personalized web that they do not think consumers are competent to decide to reject it."); *Self-Regulation Hearing*, *supra* note 10 (written testimony of Bob Liodice, President and Chief Executive Officer, Association of National Advertisers, Inc.), *available at* http://www.ana.net/getfile/17771 ("More than one million consumer opt outs have been registered under the DAA Principles since January 2011."). This represents less than 0.4 percent of people in the U.S.

[114] *See* Alex Fowler, *Mozilla Led Effort for DNT Finds Broad Support*, MOZILLA (Feb. 23, 2012), http://blog.mozilla.org/privacy/2012/02/23/mozilla-led-effort-for-dnt-finds-broad-support ("[T]he W3C . . . has a vital role to play in creating an international standard for Do Not Track that represents the consensus of a broad group of stakeholders."); *Tracking Protection Working Group*, W3C, http://www.w3.org/2011/tracking-protection/ (last visited Sep. 28, 2012) ("The Tracking Protection Working Group is chartered to improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking and for block or allowing Web tracking elements. The group seeks to standardize the technology and meaning of Do Not Track, and of Tracking Selection Lists.").

[115] *See* Wendy Davis, *FTC Defends W3C's Do-Not-Track Initiative To Congress*, ONLINE MEDIA DAILY (Sept. 27, 2012, 6:27 PM), http://www.mediapost.com/publications/article/183963/ftc-defends-w3cs-do-not-track-initiative-to-congr.html#axzz2NUEKVxxh ("Federal Trade Commission Chairman Jonathan Leibowitz told Congress this week that the agency supports the efforts of the standards group World Wide Web Consortium, which is developing voluntary guidelines for a do-not-track system.").

[116] 15 U.S.C. § 45(a)(1) (2006) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."). The power of the FTC to initiate an enforcement action against acts which it has reason to believe violate 15 U.S.C. § 45(a)(1) is called its section 5 authority because it comes from section 5(a) of the FTC Act. *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N, http://www.ftc.gov/ogc/brfovrvw.shtm (last modified July 2, 2008).

constitute a valid expression of consent.[117] This debate might benefit from drawing on the experience of the law in determining what constitutes valid consent to be bound to an online contract.

¶63 This section proceeds in three subparts. The first subpart engages the legal literature on the objective theory of contract online. The second subpart points out inconsistencies in the subjective standard endorsed by the TPE. The third subpart will engage the literature of consent as it applies to mass-market online boilerplate and will argue that advertisers are drawing on this pro-consumer literature to harm consumers.

1. The Objective Standard of Consent in Online Contracting

¶64 There is an established literature on consent in online contracting.[118] The literature has its own debates.[119] For example, the literature debates the merits of the objective and subjective theories of contractual consent.[120] However, the TPE standard lies well outside the contours of that literature, as this section explores.

¶65 The legal literature broadly agrees that the standard for online contracting must be some flavor of objective.[121] Pure subjective preferences are too easy to manipulate.[122] Thus, for example, secret preferences are not enforced because they have not been communicated to the other party.[123] This principle yields the basic balance between subjective and objective preferences in contract law. While contract law is a means of satisfying subjective preference, parties are bound to the objectively discernible meaning of their statements of preference.[124] To do otherwise would be to render contracts

---

[117] *See* Stephanie Mlot, *Google Chrome Adds Support for 'Do Not Track'*, PC MAGAZINE (Sept. 14, 2012, 5:13 PM), http://www.pcmag.com/article2/0,2817,2409764,00.asp ("Silence isn't consent in other parts of life and it shouldn't be construed as consent on the Web." (quoting ioer…@gmail.com, Comment to *Issue 81844: Implement Do Not Track*, CHROMIUM (Sept. 25, 2011), https://code.google.com/p/chromium/issues/detail?id=81844) (internal quotation marks omitted)).

[118] *See* Hannah Yee Fen Lim, *Who Monitors the Monitor? Virtual World Governance and the Failure of Contract Law Remedies in Virtual Worlds*, 11 VAND. J. ENT. & TECH. L. 1053, 1062 (2009) ("[T]he literature on consent in contracting has traditionally focused on a party's comprehension of the terms of the contract or the presence or absence of true consent in standard form contracts.").

[119] *See* Radin, *supra* note 9, at 620 ("Even when there is no signature, such as when we click 'I agree' online, courts are likely to find that a contract has been formed unless there is some other reason for invalidating the terms. Boilerplate has really come into its own in the online environment." (footnote omitted)).

[120] *See id.* at 622 ("Our courts consider boilerplate schemes contractual, but should they?").

[121] *See* Joseph M. Perillo, *The Origins of the Objective Theory of Contract Formation and Interpretation*, 69 FORDHAM L. REV. 427, 476–77 (2000); *see also* Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1311–12 (2005) ("For more than a century, courts have adhered to the objective theory of contract, which holds that the actual state of mind of the parties is irrelevant. Courts judge the conduct of contracting parties by a standard of reasonableness and find mutual agreement if a reasonable person would be led to believe that an agreement exists." (footnote omitted)).

[122] *See* Perillo, *supra* note 121, at 477 ("The reason for the persistence of objective approaches can be found in the legal profession's distrust of the testimony of parties. . . . When legislatures overturned [rules forbidding party testimony] in the nineteenth century, the profession, acting through the courts, made party testimony of intention irrelevant, giving birth to the modern objective theory.").

[123] *See* Randy E. Barnett, *The Sound of Silence: Default Rules and Contractual Consent*, 78 VA. L. REV. 821, 858–59 (1992) ("[T]he purpose for which we adopt the objective approach [is] to enable persons to rely on the appearances created by others because subjective intentions are generally inaccessible . . . . [I]n contract law, we protect a party's reliance on objective appearances, unless it can be shown that the parties shared a common subjective understanding of the term.").

[124] *See* Moringiello, *supra* note 121 at 1316 ("In the Internet age, sometimes an offeror asks an offeree to

useless. One party could always claim that she did not truly mean what was in the contract. For these reasons, the objective theory of contract appears to predominate in questions of online, mass-market consumer contracting.[125] The objective theory carries significant weight in black-letter pre-internet statements of contract law as well.[126] Courts have tended toward the objective theory of consent for reasons of discernment and administrability.[127]

¶66 This article also tends toward the objective theory of contract because objective interpretations of contracts reduce transaction costs. Yet one need not wholeheartedly endorse the objective theory of contract to criticize the one-sided application of the TPE standard. Objective or subjective, the same standard should be applied to both consumers and corporations. As the following section indicates, the TPE does not do so.

2. The TPE Standard is Doubly Subjective

¶67 The bespoke TPE standard is both inconsistent as applied to consumers,[128] and doubly subjective, in that it relies both on the user's state of mind[129] and the corporation's suspicions about the user's state of mind to trump an objective, clear term.[130]

---

assent to terms by clicking an 'I agree' icon. That click can clearly constitute a signature . . . , but the definition of 'signature' requires that the click be adopted with an *intent* to sign the contract. As result judges must ask whether or not the click through requirement sends the same clear signal, triggering the duty to read, as the paper signature requirement." (footnotes omitted)).

[125] *See* Hartzog, *supra* note 4, at 1643 ("The parties' state of mind during the formation of these agreements is irrelevant. Rather, courts consider what the parties objectively conveyed to each other in what is known as the 'objective theory of contract.' Only external acts and manifestations, not subjective, internal intentions, determine mutual assent to a contract." (footnote omitted)).

[126] *See* Perillo, *supra* note 121; RESTATEMENT (SECOND) OF CONTRACTS § 3 & cmt. b (1981) (contracts determined by external manifestation of intent); *id.* § 4; *id.* § 5 ("A term of a contract is that portion of the legal relations resulting from the promise or set of promises which relates to a particular matter, whether or not the parties manifest an intention to create those relations"); *id.* § 18 cmt. c ("If one party is deceived and has no reason to know of the joke the law takes the joker at his word."); *id.* § 19(1) ("The manifestation of assent may be wholly or partly by written or spoken words or by other acts or by failure to act"); *id.* § 19(3) ("The conduct of a party may manifest assent even though he does not in fact assent."). *But see id.* § 19 cmt. c ("A 'manifestation' of assent is not a mere appearance . . . . There must be conduct and a conscious will to engage in that conduct."). For an application of the objective theory to consumer form contracts, see generally Michael I. Meyerson, *The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 U. MIAMI L. REV. 1263 (1993).

[127] *See, e.g.*, Daniel J. Bussel & Kenneth N. Klee, *Recalibrating Consent in Bankruptcy*, 83 AM. BANKR. L.J. 663, 670 n.25 (2009) ("Today a court generally restricts its attention to the outward behavior of the parties: the meaning of their acts is not what either party or both parties intended but the meaning which a 'reasonable man' puts on these acts; the expression of mutual assent, not the assent itself, is usually the essential element." (quoting Zell v. Am. Seating Co., 138 F.2d 641, 646 (2d Cir. 1943)). *Zell* was overturned by *American Seating Co v. Zell*, 322 U.S. 709 (1944), on the grounds that it violated state parol evidence rules, but the court reasoning relating to contract interpretation stands.

[128] *Compare W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user."), *with* Nehf, *supra* note 4 ("If consumers are aware of their privacy concerns and deem privacy important, they are more likely to take steps to protect their own interests—for example, avoiding firms that might compromise their privacy interests and frequenting the ones that are more likely to protect them."); Hachamovitch, *supra* note 4 ("[W]e think . . . consumers will favor products designed with their privacy in mind over products that are designed primarily to gather their data."); *and* Nehf, *supra* note 4 ("[R]esearch on bounded rationality and consumer decision making suggests that in most circumstances consumers, acting rationally, do not factor privacy policies into their decision processes . . . . [T]he research suggests that the problem is not solvable by reducing transaction costs and making information about privacy practices more visible or easily understood.").

¶68 The TPE bespoke standard requires that a consumer prove to a web server that she specifically understood and intended to set the flag, in order for the term to be enforceable.[131] The TPE requires that the setting of the flag must be the result of informed, deliberate choice.[132] The standard permits corporations to ignore the flag if they suspect that the consumer did not intend to set the flag that the browser sent.[133] Compliance thus depends on the advertiser's subjective valuation of the consumer's subjective knowledge and consent.[134]

¶69 This introduces a standard of actual, subjective knowledge and proof of intentionality as the benchmark for consumer preference expression. The TPE bespoke standard uses the requirement of user choice as a barrier to preference expression, instead of as a means of achieving preference expression. No bespoke action is required for the consumer to consent to tracking.[135] The TPE bespoke standard thus endorses a subjective standard of actual knowledge and intentionality, but only when the consumer wants to protect her privacy, not when she wants to give her information away.[136]

3. The TPWG Standard is Inconsistently Subjective

¶70 If the standard for online consent were subjective, and if that standard were applied consistently, consumers could benefit.[137] If courts enforced subjective intentions over objective terms, consumers would be bound by fewer website Terms of Use. Consumers would be freed from browsewrap privacy policies that corporations currently use to

[129] *See W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a *deliberate* choice by the user." (emphasis added)).

[130] *See id.* ("[A] tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed."). *But see Do Not Track Us*, *supra* note 4 ("Do Not Track provides users with a single, simple, persistent choice to opt out of third-party web tracking.")

[131] *See W3C TPE Draft*, *supra* note 5.

[132] *See id.* ("[A] tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.").

[133] *See id.* ("The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed."); E-mail from ifette@google.com to Dan Auerbach, Staff Technologist, Electronic Frontier Foundation (Oct. 17, 2012, 1:09 PM), *available at* http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0302.html ("[I]f DNT does not reflect a user's preference, then there is simply no reason to adhere to it regardless of the signal's deployment. Advertisers won't care, so ad networks won't care; the existing opt-out mechanisms are more accurate than an invalid DNT signal.").

[134] *See W3C TPE Draft*, *supra* note 5; Auerbach, *supra* note 133.

[135] *See* Auerbach, *supra* note 133; *see also* John Simpson, Comment to *Do-Not-Track Community Group*, W3C (Jan. 14, 2012), http://www.w3.org/community/dntrack/ ("If DNT=1, site MUST send response header (for compliance validation) (if no response header sent, this would mean non-compliance . . . .)").

[136] *Compare W3C TPE Draft*, *supra* note 5 ("The goal of this protocol is to allow a user to express their personal preference regarding tracking to each server and web application that they communicate with via HTTP . . . . Key to that notion of expression is that the signal sent MUST reflect the user's preference . . . ."), *with* Perillo, *supra* note 121, at 427 ("By giving effect to the parties' intentions, the law of contracts is based on respect for party autonomy. Nonetheless, the objective theory of contract formation and interpretation holds that the intentions of the parties to a contract . . . are to be ascertained from their words and conduct rather than their unexpressed intentions.").

[137] *See* Radin, *supra* note 119, at 620–24 (hypothesizing a separation between contract law, governed under traditional notions of consent, and regulation of boilerplate, which has a strained relationship with traditional notions of consent).

justify tracking—policies that consumers do not read, understand, or desire.[138] People would be bound only by the terms that they understood and specifically chose. That is not this world, but it is a nice one. Yet tellingly, that is precisely what the TPE bespoke standard does not do. It instead uses the usual objective rules to tell companies that they may track, and only introduces subjectivity as grounds to doubt that a consumer means what she says.

¶71 This article therefore criticizes the TPE standard both for inconsistency and for excess subjectivity. The TPE standard applies a bespoke, subjective theory of contract consent[139] when that theory will hurt consumers by raising transaction costs for their expressions of preference,[140] but applies a standardized, objective theory of consent when that theory would help corporations. As things stand, the dividing line is not between objective and subjective, but between consumer and corporate power.

¶72 The standard for Do Not Track should not be selectively based on whether a consumer or a corporation offers the term.[141] Consumers should not be bound by silence when agreeing to corporate terms, but required to take bespoke steps to bind corporations to consumer terms. To show the logical flaw in another way, assume that the TPE bespoke standard for subjective intentionality were the online rule. One might think that advertisers would be deeply concerned. If enforceability rides on subjective preference and not on objectively expressed terms, people who enable the tracking flag to objectively indicate that tracking is acceptable, but subjectively intend not to be tracked, would pose a serious threat to advertisers. In that case, tracking would be impermissible even though the advertiser had received the "all clear" from the user's browser.

---

[138] *See, e.g.*, *Spotify Privacy Policy*, SPOTIFY (Feb. 19, 2013), http://www.spotify.com/us/legal/privacy-policy/ ("When you sign up for the Service, we may collect information we ask you for, like your username, password, e-mail address, date of birth, gender, postal code, and country. We may also collect information you voluntarily add to your profile, such as your mobile phone number and mobile service provider. If you connect to the Service using your Facebook credentials, you authorise us to collect your authentication information, such as your username, encrypted access credentials, and other information that may be available on or through your Facebook account, including your name, profile picture, country, hometown, e-mail address, date of birth, gender, friends' names and profile pictures and networks. We may store this information so that it can be used for the purposes explained in Section 3 and may verify your credentials with Facebook.); *see also* Complaint, Kim v. Space Pencil, Inc., No. CV-11-3796 (N.D. Cal. Aug. 1, 2011); Hoofnagle et al., *supra* note 4, at 292 ("The KissMetrics system presents another problem, in addition to a lack of notice and invalidation of choice. It allows companies to aggregate information about users in new ways that consumers are unlikely to understand.").

[139] *See W3C TPE Draft*, *supra* note 5 ("The goal of this protocol is to allow a user to express their personal preference regarding tracking . . . . Key to that notion of expression is that the signal sent MUST reflect the user's preference, not the choice of some vendor, institution, site, or any network-imposed mechanism outside the user's control.").

[140] *See* Kesan & Shah, *supra* note 4, 601–02*; see also* Leon, *supra* note 2, at 597 ("If a user proactively downloads a browser add-on like Ghostery or TACO, or proactively visits an opt-out website, their action indicates that they likely intend to block tracking. However, Ghostery and TACO do not block any trackers by default, and enabling tracking involves multiple clicks."); Riva Richmond, *Resisting the Online Tracking Programs*, N.Y. TIMES, Nov. 10, 2010, http://www.nytimes.com/2010/11/11/technology/personaltech/11basics.html ("Keeping your computer free of tracking programs is not easy . . . . A number of tools can *minimize* tracking, but using them requires considerable effort and tech know-how." (emphasis added)).

[141] *See W3C TPE Draft*, *supra* note 5 ("[A] tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.").

¶73 Online contracts do not and cannot function in this manner. Parties to online contracts exchange standardized language all the time.[142] There is little inquiry as to whether the parties truly wanted, explicitly intended, or even bothered to read each clause.[143] Online parties are bound to the objective meaning of communicated terms. Mainstream contract theory certainly does not require that online parties read, or somehow explicitly adopt by deliberate choice, their contractual terms by some act beyond communicating them to the other party.[144] Were that the standard, no online contract would stand, since vanishingly few of them are read by anyone.[145] With some exceptions for unconscionability, parties to online contracts are bound to what they would have understood had they read the terms.[146]

¶74 Corporate webservers automatically communicate legal terms of service and end user license agreements (TOS's and EULAs) to consumers all the time.[147] There is no reason that a consumer cannot communicate terms to the corporation in exactly the same fashion.[148] There is no reasonable unconscionability attack on a consumer's statement that she does not desire to be tracked. All that is missing is a technological means of automatically communicating that contractual term to the corporation. That is what Do-Not-Track is, in the legal sense. It communicates the critical term that matters to a customer. The Do-Not-Track flag indicates to the corporation that if the corporation wishes to do business with the consumer, it must do so without tracking.

---

[142] *See* Becher & Zarsky, *supra* note 72, at 305 ("For many decades, numerous consumer transactions . . . have [occurred] through, standard form contracts ("SFCs"). Form contracting will presumably continue to predominate, as modern technology and recent developments bring new and improved standard contracting practices into the market. One prominent example is online contracting . . . .").

[143] *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 466 (2006) ("Clickwraps put some pressure on the classical notion of assent derived from bargained agreements, because they substitute a blanket, take-it-or-leave-it assent for the classical notion that the parties actually thought about and agreed to the terms of the deal.").

[144] *See W3C TPE Draft*, *supra* note 5 ("The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user."); Randy E. Barnett, *Consenting to Form Contracts*, 71 FORDHAM L. REV. 627, 635 (2002) ("Now think of click license agreements on web sites. When one clicks "I agree" to the terms on the box, does one usually know what one is doing? Absolutely. There is no doubt whatsoever that one is objectively manifesting one's assent to the terms in the box, whether or not one has read them.").

[145] *See* Hartzog, *supra* note 107, at 1642 ("It has become a truism that virtually no one reads standard-form online agreements.").

[146] *See* Nathan J. Davis, Note, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 579 (2007) ("[A]bsent fraud or deception, the user's failure to read, carefully consider, or otherwise recognize the binding effect of clicking 'I Agree' will not preclude the court from finding assent to the terms.").

[147] *See, e.g.*, MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 935 (9th Cir. 2010) ("Each WoW player must read and accept Blizzard's End User License Agreement ('EULA') and Terms of Use ('ToU') on multiple occasions."), *amended by denial of reh'g*, No. 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011); Kloth v. Microsoft Corp., 444 F.3d 312, 318 (4th Cir. 2006) ("To use Microsoft software, the end-users were required to agree to the EULAs, which provided, among other things, a Microsoft-funded refund to the end-user if the end-user declined to enter into the EULA.").

[148] *See* Fairfield, *supra* note 27, at 581–84; *see also* Dusollier, *supra* note 105 (discussing that the purpose of Creative Commons is to address the over-expansion of copyright and rebalance in favor of future creators and users of copyrighted works).

4. The Boilerplate Literature

¶75 An overlapping literature discusses the impact of boilerplate on consent theory.[149] This literature is related to the discussions of the objective theory of contract, but has its own history. Boilerplate is ubiquitous online, and it is often used in situations marked by disparate bargaining power.[150] The dominance of online boilerplate raises serious questions as to whether the consumer has given any meaningful consent.[151]

¶76 As with the discussion of objectivity and subjectivity above, the opponents of default Do-Not-Track draw on the language of consumer protection.[152] Advertisers argue that consumer-offered standardized contracts should not be enforced, using arguments that consumer advocates developed to explain why corporate-offered standard contracts should not be enforced.[153] The advertising industry thus uses pro-consumer arguments against consumers.

¶77 Consumer advocates should continue to challenge whether consumers meaningfully consent to corporate-proffered contracts. But that has nothing to do with whether consumers consent to consumers' own terms. That would read the literature backwards. The boilerplate literature nowhere asserts that corporations are not bound by the terms they themselves offer. Much the contrary: when a rare term that benefits consumers appears in a corporate-drafted contract, the corporation is held to the very jot and tittle of its statement.[154]

¶78 The other reasons for concern over consent to boilerplate do not appear to apply, either. Common criticisms of corporate-drafted contracts are that they exploit asymmetric bargaining power through the consumers' economic need or the corporations' dominant market position, or that such contracts exploit information asymmetry because the contracts are long and complicated.[155] These reasons are not

---

[149] *See, e.g.*, Florencia Marotta-Wurgler, *What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements*, 4 J. EMPIRICAL LEGAL STUD. 677, 678 (2007) (addressing the lack of consumer choice in accepting boilerplate language in standard form contracts).

[150] *See* Knapp, *supra* note 107; Lemley, *supra* note 143, at 459 (2006) ("Today, by contrast, more and more courts and commentators seem willing to accept the idea that if a business writes a document and calls it a contract, courts will enforce it as a contract even if no one agrees to it.").

[151] *See* Lemley, *supra* note 150 ("Clickwraps put some pressure on the classical notion of assent derived from bargained agreements, because they substitute a blanket, take-it-or-leave-it assent for the classical notion that the parties actually thought about and agreed to the terms of the deal.").

[152] *See W3C TPE Draft*, *supra* note 5 ("The goal of this protocol is to allow a user to express their personal preference regarding tracking . . . . Key to that notion of expression is that the signal sent MUST reflect the user's preference . . . ."); Julia Angwin, *supra* note 14 ("Stu Ingis, general counsel of the [Digital Advertising Alliance] . . . . said that the industry supports 'consumer choice, not a choice made by one browser or technology vendor.'"); *see also* Shankland, *supra* note 3 ("Roy Fielding, an author of the Do Not Track (DNT) standard and principal scientist at Adobe Systems, wrote a patch for Apache . . . that sets the Web server to disable DNT if the browser reaching it is Internet Explorer 10. 'Apache does not tolerate deliberate abuse of open standards,' Fielding titled the patch.").

[153] *See supra* subparts II.C.1–3.

[154] *See* Yellowbook Inc. v. Brandeberry, 708 F.3d 837, 847 (6th Cir. 2013) (discussing *contra proferentem*, the canon of construction interpreting contract terms against the drafter: "[T]he '*contra proferentem*' canon is meant primarily for cases 'where the written contract is standardized and between parties of unequal bargaining power.'" (quoting Savedoff v. Access Group, Inc., 524 F.3d 754, 764 (6th Cir. 2008))).

[155] *See* Shmuel I. Becher, *Asymmetric Information in Consumer Contracts: The Challenge that is Yet to be Met*, 45 AM. BUS. L.J. 723, 734 (2008) ("The existence of obligational asymmetric information is a serious market failure that can undermine the efficiency of many consumer transactions."); Russell

present when one considers a simple, consumer-offered Do-Not-Track term. Consumers offer no economic coercion. They have no monopoly. A Do-Not-Track term is not prolix or obfuscatory, unlike corporate boilerplate.

¶79 Consumer advocates should try to put the power of automated, standardized contracts into consumers' hands.[156] Standardized contracts in consumers' hands are different from standardized contracts in corporate hands. When a consumer proffers a standardized contract, she is expressing a preference. No one would think a corporation was not expressing a contractual preference if it offered automated terms via webservers. The same should be true of consumers offering terms through web browsers.

¶80 It is understandable that legal academics resist corporate boilerplate terms by questioning whether consumers meaningfully consent to corporate-drafted contracts. But arguments about why consumers do not consent to corporate terms do not apply to a discussion of whether consumers consent to their own terms. Arguments about consent are being misused to prevent consumers from benefiting from asserting their own boilerplate terms. That was not what consumer advocates meant when they critiqued consent in boilerplate, nor should it be used here to stop consumers from benefitting from their own automated, default legal terms telling companies not to track.

5. Political Impact of Mistakes in Contract Theory

¶81 The advertising industry continues to assert that compliance with the Do-Not-Track standard is voluntary.[157] That is only true to the extent that compliance with any valid contract term is voluntary. If a consumer offers to do business on the condition that she is not tracked, and the advertiser proceeds to do business with the consumer based on that knowledge, the advertiser has accepted that term.[158] The term is as binding as any that the web server might convey to the consumer. The advertiser cannot plead ignorance and proceed as if the advertiser had received permission to track.

¶82 A consumer contractual term stating, "If you (corporation) want to do business with me, you may not track me," is, without question, enforceable. A breach of that promise is a breach of contract and an unfair business practice. In insisting on their right to ignore consumers' facially valid Do-Not-Track flags, advertisers follow a dangerous path. There is no legal difference between a corporation asserting in its privacy policy that it will not track, and a corporation's acceptance of a consumer's term that bars tracking.[159]

Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L.R. 1203, 1233–34 (2003) ("[I]t is not difficult to explain the common observation that buyers rarely read the terms in form contracts. It is not simply the fact that reading the terms (and sometimes understanding them) is time-consuming . . . although it is no doubt true that in some cases the time investment required outweighs the benefits . . . ." (footnote omitted)).

[156] *See* Radin, *supra* note 9.

[157] *See, e.g.*, Todd R. Weiss, *Google Adding 'Do No Track' Into Chrome's Latest Developer Build*, EWEEK (Sept. 16, 2012), http://www.eweek.com/c/a/Security/Google-Adding-Do-No-Track-Into-Chromes-Latest-Developer-Build-852453/ ("Do Not Track controls built into Web browsers only have to be complied with by Websites and advertisers on a voluntary basis because there are no laws or requirements that control such information today.").

[158] *See* Fairfield, *supra* note 27 ("When a consumer expresses her preference, in the very first exchange between the consumer and corporate computers, for the corporation not to track her information, the company is free to refuse the transaction if it does not wish to continue on the consumer's terms.").

[159] *See* Hartzog, *supra* note 4, at 1643 ("When a website contains the phrase, 'we respect your privacy,'

Both are contractual consumer-facing promises; both are equally valid and enforceable. Online advertisers that ignore Do-Not-Track flags breach numerous privacy contractual promises every day. Corporations have been given some leeway to self-regulate, but instead of seizing that opportunity, many have chosen to undermine the DNT standard, perhaps hoping to avoid regulation while ensuring that the standard provides consumers little meaningful protection.[160]

¶83 The FTC has for the time being chosen to let the self-regulatory process work itself out.[161] Waiting on self-regulation is perhaps wise politics, but it is wise politics only for the FTC, not for the advertisers that ignore DNT flags and the consumers who continue to be tracked against their wishes. If the Do-Not-Track standard produces a real standard that protects consumers, the FTC receives the benefit of a strong rule without appearing interventionist. If the debate over default Do-Not-Track scuttles the Do-Not-Track effort,[162] the FTC will be able to point to repeated industry failures to implement even the most radically simple consumer protection. Further, the FTC has not hesitated in the past to enforce consumer-facing privacy promises against companies that violate them.[163] Should the self-regulatory process fail, it could certainly do so in the case of ignored DNT flags.

III. WHY PRIVACY MUST BE AUTOMATED

¶84 This section turns from the discussion of default DNT and the TPE bespoke standard to a broader discussion about automation and privacy. It makes two arguments. First, it argues that substantive theories of privacy must be considered especially suspect

---

it does not matter what the website intended. The question is what a reasonable person in the user's position would have understood from that communication." (footnote omitted)); Fairfield, *supra* note 158; s*ee also* E-mail from Peter Cranstone to W3 Tracking (June 20, 2012, 8:23 AM) (http://lists.w3.org/Archives/Public/public-tracking/2012Jun/0556.html) ("The expectation of a binary protocol (DNT:1) is very simple. It means what it says from the users perspective. It's now time to align that with the decisions made by the server. I doubt failure is going to be an option in this case.").

[160] *See* Shankland, *supra* note 3 ("'If the site does not believe the DNT:1 signal is valid, then why would anyone in the supply chain be expected to honor the invalid signal?' asked Mike Zaneis, general counsel of the Internet Advertising Bureau in a comment on the DNT standard.").

[161] *See Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 41, at 3 ("As part of the call for simplified choice, staff asked industry to develop a mechanism that would allow consumers to more easily control the tracking of their online activities, often referred to as 'Do Not Track.'").

[162] *See* James Temple, *Is 'Do Not Track' Dead?*, SFGATE (Oct. 11, 2012, 4:53 PM), http://www.sfgate.com/technology/dotcommentary/article/Is-do-not-track-dead-3940805.php ("After months of occasionally constructive discussions to define what it should mean when consumers flip on a 'do not track' switch in Web browsers, advertising lobbyists threw the talks into disarray last week by advancing an outlandish proposal . . . . [T]he Digital Advertising Alliance and Association of National Advertisers pushed to exempt from the rules all online marketing and advertising—the issue at the heart of the debate.").

[163] *See, e.g.*, Federal Trade Commission v. Toysmart.com, LLC, Civ.A. No. 00-CV-11341-RGS, slip op. at 1 (D. Mass. Aug. 21, 2000) (alleging that Toysmart engaged in deceptive acts or practices in violation of section 5 of the Federal Trade Commission Act when it violated the terms of its privacy policy with consumers about disclosure of personal information and therefore engaged); *FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, FTC (July 21, 2000), http://www.ftc.gov/opa/2000/07/toysmart2.shtm ("In a settlement announced today by the Federal Trade Commission, Toysmart.com ('Toysmart') has agreed to settle charges the company violated Section 5 of the FTC Act by misrepresenting to consumers that personal information would *never* be shared with third parties and then disclosing, selling, or offering that information for sale in violation of the company's own privacy statement.").

when their implementation actively increases the transaction costs involved in protecting privacy.[164] Second, it asserts that only automated features can sufficiently reduce consumer privacy transaction costs such that one might assess the contours of a market for privacy platforms. It concludes that advertising industry advocates do not embrace free-market principles, but rather seek to prevent products with innovative privacy features like default DNT from reaching the market.

A. Transaction Costs and Bespoke Contract Terms

¶85 This section explores the implications for models of privacy should consumers be required to manually set privacy preferences. In so doing, the section hopes to establish why the fight over privacy should turn on the basic question of how much time and money it costs consumers to obtain privacy, instead of continuing to ask what privacy is, or whether consumers actually want it.

¶86 Consumers are often denied the ability to offer their own contract terms when they contract online. For example, a consumer term might be ignored under the standard established in *ProCD, Inc. v. Zeidenberg*[165] and *Hill v. Gateway*.[166] More often, though, consumers are denied the ability to set their own terms online as a matter of design. Websites and e-commercial forms do not contain any way for consumers to offer their own terms.[167] Online forms carefully control what the consumer is allowed to express. In most online transactions, consumers may only specify how many of a good they wish to order. Other terms such as warranties, remedies, or limitations are not negotiable because the mechanics of the online form lack such affordances.[168]

¶87 The most common rationale for denying consumers the right to introduce contract terms is that doing so would raise transaction costs online.[169] There is developed

---

[164] *See* McDonald & Cranor, *supra* note 73 ("Privacy policies should help reduce information asymmetries because companies share information with their customers . . . . [but] if the cost for reading privacy policies is too high, people are unlikely to read policies."); *see also* Jeff Sovern, *Toward a New Model of Consumer Protection: The Problem of Inflated Transaction Costs*, 47 WM. & MARY L. REV. 1635, 1637 (2006) ("In many circumstances, businesses benefit by increasing consumer transaction costs to the detriment of consumers . . . . [S]ome practices are profitable largely because they inflate consumer transaction costs . . . . [F]irms increase consumer transaction costs because doing so enriches them.").

[165] *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) ("Our case has only one form; UCC § 2-207 is irrelevant . . . . A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance. And that is what happened.").

[166] *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149 (7th Cir. 1997) ("Plaintiffs ask us to limit *ProCD* to software, but where's the sense in that? *ProCD* is about the law of contract, not the law of software.").

[167] *See* Ichiro Kobayashi, *Private Contracting and Business Models of Electronic Commerce*, 13 U. MIAMI BUS. L. REV. 161, 184 (2005) ("Electronic commerce is so standardized and automated that understanding the total mechanism of a business model is important. A transaction in an electronic commerce business model is created in a conveyer-belt style of machine-made, automated contract-formation process, where "electronic agents" are actually engaged in negotiating with consumers.").

[168] *See* Knapp, *supra* note 107 (discussing how dominance of the drafter has become typical in contract law); Lemley, *supra* note 143, at 459 ("Today, by contrast, more and more courts and commentators seem willing to accept the idea that if a business writes a document and calls it a contract, courts will enforce it as a contract even if no one agrees to it.").

[169] *See* Kobayashi, *supra* note 167, at 168 (2005) ("While the rapid and standardized character of electronic commerce substantially reduces direct administration costs, substantive contract negotiations are more difficult. This means that transaction costs for executing complete contracts (contract drafting costs)

literature on the costs of bespoke contracting in online contracts.[170] Bespoke contract terms raise transaction costs.[171] If consumers (or any contracting party online) were free to add individuated, customized clauses to every contract online, the transaction costs for businesses would rise significantly. Businesses would be required to read each contract to ensure that the term modified by the consumer would not scuttle the deal.

¶88 For this reason, courts prefer standardized contracts over bespoke terms.[172] Yet the problem stems from bespoke terms,[173] rather than customer-proffered terms.[174] Whether a term is bespoke or standardized impacts transaction costs. Whether a term is offered by a corporation or a consumer does not. In the case of Do-Not-Track, it is the consumer who offers a standardized term.

¶89 The advertising industry attempts to confuse the meaning of a facially valid Do-Not-Track flag by insisting that only those flags that the consumer subjectively desires should be enforceable.[175] Conditioning enforcement on subjective and bespoke terms should be the last thing advertisers want. Suppose courts actually enforced idiosyncratic, subjective consumer preferences in mass-market contracts. By advocating for a bespoke standard, advertisers would do themselves grave economic harm. They would be bound to those terms the consumer subjectively desired, regardless of objective appearances. They would be bound by idiosyncratic terms, regardless of the existence of a standard.

¶90 Do-Not-Track is a standardized, objectively clear term. If advertisers left the meaning of the flag alone, compliance costs with the flag would be near-zero. Once the flag is communicated, the corporation may not track. There need be no complicated meta-analysis in which the corporation ignores the facially valid flag because it can manufacture doubt about what the consumer subjectively wanted. If a corporation

---

are relatively high."); *see also* McDonald & Cranor, *supra* note 73, at 564.

[170] *See* Henry E. Smith, *Modularity in Contracts: Boilerplate and Information Flow*, 104 MICH. L. REV. 1175, 1210 (2006) ("The use of boilerplate thus lowers legal costs, in part because it is simple and in part because this simplicity through modularity allows its reuse."); Joshua Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1401, 1405 (2009) ("If standardized deals lower information costs, customized deals may raise them. . . . [C]ustomized deals that economic theory has long considered efficient instead increase information costs for third parties and thus can be suboptimal across the run of mass-market contracts.").

[171] *See* Robert B. Ahdieh, *The Strategy of Boilerplate*, 104 MICH. L. REV. 1033, 1034 (2006) ("[R]eliance on standard terms may minimize the transaction costs of drafting and negotiating contract terms.").

[172] *See* Fairfield, *supra* note 170, at 1451 ("Despite court rhetoric disfavoring standardized agreements, some courts protect standardized deals by using anti- standardization doctrines to strike outlier terms.").

[173] *See supra* note 170 and accompanying text.

[174] *See* Radin, *supra* note 9 ("Is it possible to use automation to enable consumers to get terms they would actually prefer? There are a few possibilities. . . . Online systems could . . . enable users to customize their own terms. . . . Filtering systems on personal computers would be market solutions because computer users would be free to use them or not use them . . . .").

[175] *See* E-mail from Chris Mejia to W3C DNT Working Group Mailing List (May. 30, 2012, 7:34 PM), http://lists.w3.org/Archives/Public/public-tracking/2012May/0322.html ("If the user's intent in turning on/off DNT is not clear . . . , there is no way for publishers to understand how to accurately 'honor' any consumer's DNT header flag . . . ."); E-mail from Mike Zaneis to David Singer (Aug. 23, 2012, 7:28 PM), http://lists.w3.org/Archives/Public/public-tracking/2012Aug/0168.html ("[If] the user visits a site, and the user-agent sends a DNT header, but the site isn't sure it reflects the user's true intentions . . . . [the site] . . . might be concerned that, in this case, the site's chosen 3rd parties will be asked not to track when that was not the user's true request."); E-mail from Shane Wiley to Walter van Holst (Nov. 7, 2012, 1:06 PM), http://lists.w3.org/Archives/Public/public-tracking/2012Nov/0085.html ("If servers have no confidence that USERS are directly activating DNT, they will not implement DNT . . . .").

receives a DNT flag and cannot function without tracking, the simplest expedient would be for the corporation to refuse access to the consumer, as some sites do to surfers who disable cookies.

¶91 Bespoke clauses not only raise transaction costs individually, but also raise transaction costs in the aggregate. The simple reason privacy policies have failed is that there are too many of them for consumers to read,[176] as the transaction costs of interacting with counterparties are multiplied by the number of counterparties. These costs are, in the aggregate, too much for consumers to pay.[177] The basic logical failure of the current privacy framework lies in considering the cost of each privacy feature alone, rather than the cost of privacy in the aggregate. Reading one privacy policy might not be too much to ask. Reading hundreds of thousands of privacy policies is impossible.[178]

¶92 Similarly, setting one privacy flag might not be too much to ask. To ask consumers to understand and configure increasing numbers of privacy features by hand is, in the aggregate, to condemn them to failure.[179] Privacy enhancements must multiply as means of invading privacy multiply. If each marginal privacy-invading feature can be automated while each marginal privacy-protecting feature must be hand-configured, consumers will lose.[180] Skewing the transaction costs skews the market for privacy features.

¶93 The best way not to be tracked is to choose and use a browser that does not permit tracking through a constantly expanding suite of automated, integrated features. The value of an integrated privacy-protecting browser is that all of the settings, by default, are pro-privacy.[181] Simplicity, and thus effectiveness, is a function of the aggregate cost of using a program, not a function of any given feature. Without integration and

---

[176] *See* Karim Z. Oussayef, *Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies*, 14 B.U. J. SCI. & TECH. L. 104, 125 (2008) ("[C]urrent privacy policies increase the cost to the consumer in . . . selecting between online companies. . . . Considering the length and ambiguity of the policies, careful consumers would have to spend a significant amount of time combing through policies just to engage in routine online activities. Even if consumers take every precaution there no guarantee [sic] that they will not misinterpret essential language.").

[177] *Cf.* Nehf, *supra* note 4, at 4 ("[D]espite the proliferation of privacy policies online, consumers' privacy interests may in fact be no better protected today than they were ten years ago."); *see also* Cleland, *supra* note 80 ("People deserve the right to vote for themselves if they want to be tracked . . . . [R]ight now people have no real choice because the technology is way ahead of what people want and the state of the law.").

[178] *See* McDonald & Cranor, *supra* note 73, at 544–50 ("[S]tudies show privacy policies are hard to read, read infrequently, and do not support rational decision making." (citation omitted)).

[179] *See supra* notes 113 and 164 and accompanying text; *see also* Lorrie Faith Cranor, *A Framework for Reasoning About the Human in the Loop*, UPSEC'08 PROC. OF THE 1ST CONF. ON USABILITY, PSYCHOL., AND SECURITY (2008), *available at* https://www.usenix.org/legacy/events/upsec08/tech/full_papers/cranor/cranor.pdf ("With so many security failures attributed to humans, secure systems that do not rely on a 'human in the loop' to perform security-critical functions are attractive. Automated components are generally more accurate and predictable than humans, and automated components don't get tired or bored.").

[180] *See* Cleland, *supra* note 177; *see also* John C. Abell, *The Tracks of My Fears*, REUTERS (Oct. 19, 2012), http://blogs.reuters.com/mediafile/2012/10/19/the-tracks-of-my-fears/ ("Making Do Not Track voluntary means that (because we are lazy, easily distracted humans) there will be more people being tracked.").

[181] *See Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 41 ("All of the principles articulated . . . are intended . . . to shift the burden for protecting privacy away from consumers and to encourage companies to make strong privacy protections the default.").

automation, each feature may be individually simple, while the aggregate becomes unwieldy.[182]

¶94 Browsers like the TOR Browser provide the feature of simplicity, of having already integrated privacy as a guiding principle from the ground up.[183] Their value lies in the fact that one does not have to go through a complex configuration process to use them. Rather, the defaults have been set to protect privacy at each distinct level.

¶95 Insisting that privacy features be simple by design does not resolve the aggregation problem. This explains why regulatory memes like "privacy by design" have had limited success in convincing companies dependent on advertising revenue to design products that protect consumers' privacy.[184] One example is the infamous suite of Facebook privacy controls.[185] Requiring that privacy features be included by design does not answer whether the features are useable or useful in the aggregate.[186]

¶96 Privacy by design will not succeed either as a self- or government-regulatory narrative unless it expressly incorporates aggregate simplicity as its governing principle. Privacy features must constantly expand. Unless a product with n+1, n+10, or n+100 features is precisely as simple to use as a product with n features, the aggregate cost of configuring features will alone defeat any attempt to protect privacy. The only way this can be handled is through competitive offerings of products that automate and integrate privacy features.

¶97 The ostensibly pro-market and pro-consumer-choice opponents of default DNT oppose this kind of free-market test. The function of the TPE bespoke standard is to prevent Microsoft (or any other competitor) from offering consumers a product that contains a competitive integrated and automated feature: do-not-track enabled as a default setting.[187] This makes no sense whatsoever if the industry's goal is truly to satisfy

---

[182] *See* Richmond, *supra* note 140 ("Keeping your computer free of tracking programs is not easy . . . . A number of tools can *minimize* tracking, but using them requires considerable effort and tech know-how." (emphasis added)); Leon, *supra* note 2 ("We present results of a 45-participant laboratory study investigating the usability of tools to limit online behavioral advertising . . . . None of the nine tools we tested empowered study participants to *effectively* control tracking and behavioral advertising according to their personal preferences." (emphasis added)).

[183] *See Tor Browser Bundle*, TOR PROJECT, https://www.torproject.org/projects/torbrowser.html.en (last visited Sept. 8, 2012) ("The Tor Browser Bundle lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.").

[184] *See, e.g.*, *About Adblock Plus*, ADBLOCK PLUS, http://adblockplus.org/en/about (last accessed July 12, 2013) (describing Adblock plus as a program that blocks advertisements on websites and can be modified with filters based on privacy preferences). *But see Allowing Acceptable Ads in Adblock Plus*, ADBLOCK PLUS, http://adblockplus.org/en/acceptable-ads (last visited Sep. 8, 2012) (discussing the switch in Adblock Plus 2.0 to a changeable default setting where previously disallowed non-intrusive advertisements will be allowed).

[185] *See* Jessica E. Vascellaro, *Facebook Grapples with Privacy Issues*, WSJ.COM, May 19, 2010, http://online.wsj.com/article/SB10001424052748704912004575252723109845974.html ("The social network has come under fire for a series of recent changes to its policies that have limited what users can keep private, as well as embarrassing technical glitches that exposed personal data.").

[186] *See* Jonathan Mayer, *Tracking the Trackers: Self-Help Tools*, CENTER FOR INTERNET & SOC'Y (Sept. 13, 2011, 4:35 AM), http://cyberlaw.stanford.edu/node/6730 (discussing an empirical review of tracking with the findings of: "[m]ost desktop browsers currently do not support effective self-help tools" and those that do "vary substantially in performance").

[187] *See Self-Regulation Hearing*, *supra* note 10; Ingis, *supra* note 66.

actual consumer preferences for a profit. Here, however, a group of companies seeks to stop one of its members from offering a pro-consumer privacy feature.[188]

¶98 This is anti-competitive and anti-free-market.[189] The TPE standard does not create the basis for a developing market for privacy features, as it should. Instead, The TPE establishes a punishment for those who bring new privacy features to the market: their browsers will not be protected by DNT. The standard directly prevents one of the most important privacy features from reaching the market. If the TPE bespoke standard effectively stops one privacy feature from being integrated and automated on the grounds that integration and automation do not reflect user choice, it will stop more. The effects of the TPE bespoke standard will therefore be felt well beyond the narrow range of Do-Not-Track.

¶99 Finally, the TPE bespoke standard is corrosive because it reinforces the idea that consumers are second-class citizens in the realm of online contracting. As a thought experiment, consider treating both parties to an online contract equally, each with the full power to offer and reject terms. If both corporations and consumers are forced to contract by hand online, e-commerce will grind to a halt. If both corporations and consumers are free to use software agents to automate transactions, then online transactions will proceed with lower transaction costs and a higher volume of gainful trades.[190] In no case does it make sense to give the power to offer and enforce automated contract terms to one party but deny it to the other. Yet this is precisely the state of affairs that courts and industry groups have brought about.[191] Corporations contract daily with millions of consumers by offering automated deals to purchase their private information. Yet corporations do not wish to be bound by consumers' own automated terms.

B. Establishing a Market for Privacy

¶100 It is more useful to reduce the staggering burden of consumer privacy transaction costs than it is to hypothesize about, much less set industry standards based on, any substantive theoretical model of privacy.[192] It is certainly a mistake to base legal standards on a demonstrably wrong theory of online consent. That is what the TPE

---

[188] *See* Kashmir Hill, *Microsoft is Losing in a Bitter Battle to Protect Internet Users' Privacy*, FORBES (Oct. 10, 2012, 12:57 PM), http://www.forbes.com/sites/kashmirhill/2012/10/10/microsoft-is-losing-in-a-bitter-battle-to-protect-users-privacy/ ("The Digital Advertising Alliance, a trade group that represents a bulk of Internet advertising companies, released a 'Screw you, Microsoft' statement this week, informing the tech giant that its members plan to ignore the DNT signal emitted by Internet Explorer 10 users.").

[189] *See, e.g.*, *USA: Mandatory Do Not Track Rules Re-introduced After Industry's Failure to Comply Voluntarily*, DATA GUIDANCE, http://dataguidance.com/news.asp?id=1979 (last updated July 3, 2013) ("Digital Advertising Alliance (DAA), a consortium of the US largest media and marketing associations, . . . stated: 'The DAA does not require companies to honor DNT signals fixed by the browser manufacturers and set by them in browsers.' Additionally, according to Association of National Advertisers' statement . . . , 'Apache, a provider of software that supports nearly two-thirds of internet web site offerings, has designed its software to ignore the 'do-not-track' setting if the browser reaching it is Internet Explorer 10.'").

[190] *See generally* Coase, *supra* note 63; *see also* Nehf, *supra* note 177, at 5 ("Without prohibitively high transaction costs . . . informed consumer choices should produce more efficient privacy practices online.").

[191] *See Self-Regulation Hearing*, *supra* note 10.

[192] *See* Hoofnagle et al., *supra* note 4, at 273–74, 295; Nehf, *supra* note 4, at 5; Sovern, *supra* note 164; *see also* Richmond, *supra* note 140; Leon, *supra* note 2.

bespoke standard does when it denies consumers the ability to choose pro-privacy products, in the name of protecting consumer choice.

¶101 The market for privacy features is only visible through the very dirty window of transaction costs. Some theories of privacy further muddy the window and obscure the market for privacy. Substantive theories of privacy are suspect when their implementation increases transaction costs. The view that consumer choice must be limited to a specific kind of check-the-radio-button choice, and not as to which product to use, is precisely the sort of theory that one should suspect.

¶102 It is better to reduce transaction costs and generate a true market test. A true market test would permit customers to choose between products that offer default automated privacy features, and those that offer bespoke hand-configured privacy features. But if the TPE bespoke setting becomes the industry standard, or if the FTC then tacitly adopts it as a standard against which unfair or deceptive practices are measured for purposes of section 5 of the Federal Trade Commission Act,[193] consumers will never have that choice—the bespoke standard would be the standard enforced by the FTC.

¶103 It is common to assert that privacy is dead because consumers do not succeed in protecting their privacy rights.[194] The argument is circular. Consumers do not succeed in protecting privacy, therefore they must not value privacy. Yet given the transaction costs that consumers are forced to bear to achieve any modicum of privacy protection, it is simply inaccurate to assert that consumers do not value privacy merely because they do not use tools calculated to avoid use.

¶104 For industries that oppose privacy,[195] it is much more politically effective to offer a competing high-transaction-cost substantive model of privacy, than to openly oppose consumer choice. These models then self-perpetuate because they obscure the very market that the model was meant to describe. Supporting costly choice has proven a better political strategy than openly opposing privacy.

¶105 The self-regulatory frameworks proposed by the advertising industry are grounded on a high-transaction-cost substantive privacy model. Advertisers then mistake consumer failure to overcome transaction costs for lack of a market demand for privacy.[196] For

---

[193] The argument is that acting in noncompliance with Do-Not-Track while claiming compliance is an unfair or deceptive act or practice in or affecting commerce. *See* 15 U.S.C. § 45(a)(2) (2006) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."); *see also* David Alan Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches?*, 2011 STAN. TECH. L. REV. 12, ¶¶ 30–31 (2011) ("In 2001 the federal banking agencies issued joint Interagency Guidelines Establishing Standards for Safeguarding Customer Information . . . . The following year the FTC issued its own "Safeguards Rule," which it described as an attempt to 'mirror[] the requirements of the Interagency Guidelines."). The FTC is likely to interpret advertisers' acts by reference to the self-regulatory standard. If the bespoke standard is the measuring stick by which unfair or deceptive acts are measured—that is, if it is fair to interpret a "Do-Not-Track" flag as permission to track—the FTC will have little ability to protect consumers.

[194] *See supra* note 1 and accompanying text.

[195] That advertisers oppose privacy for reasons of profit, rather than out of any malice, does not matter. Advertisers want to use all useful information. Privacy requires that they not gather or use some information from some users.

[196] *See Self-Regulation Hearing*, *supra* note 10, at 30:30 (statement of Bob Liodice, President of the Ass'n of Nat'l Advertisers) ("We believe that virtually all U.S. consumers are being exposed to the icon

example, in Senate hearings on industry self-regulation and Do-Not-Track, a speaker from the Digital Advertising Alliance claimed that a no-tracking system had been implemented by advertisers, that it was responsive to customer concerns, and that it was effective.[197] The DAA's opt-out system was supposedly offered in one trillion advertisements a month, but was used only one million times during half a year.[198] As another speaker on the same panel noted, the overall numbers indicated that the DAA's opt-out icon was used by four hundredths of one percent of consumers.[199]

¶106 These numbers drive the privacy-is-dead meme. They are also misleading, because they mistake transaction costs for lack of substantive interest in privacy. Consider several points of comparison. While the DAA Ad-option icon registers a four-hundredths of one percent use rate by consumers,[200] Mozilla has a nine percent adoption rate of users who find and set the Do-Not-Track flag in its desktop browser version, versus eighteen percent of users who find and set the Do-Not-Track flag in Mozilla's mobile version.[201] Before rolling out IE10, Microsoft's surveys indicated seventy-five percent of customers preferred not to be tracked.[202] A recent Customer Commons study found that 92% of survey respondents falsified or withheld personal information for the sake of maintaining privacy online.[203] Finally, a Pew survey indicated that sixty-eight percent of Americans are "NOT OKAY" with online tracking.[204] Either large numbers of surveyed consumers are dissembling as to their privacy preferences, or opt-out options like the DAA's Ad-option icon are hard to find and use, and are lost in the flood of other icons, seals, and marks online. The second explanation is simpler and more likely to be accurate.

¶107 In the specific case of the DAA Ad-option icon, people may not use it because they are required to click on an ad to do so. Consumers may believe that this will lead to more advertising and tracking, not less.[205] They also may not understand what the icon means. As a simple non-scientific experiment, the reader might also ask herself if she has ever seen, used, or understood the DAA Ad-option icon.[206] And that icon is just one of hundreds of privacy seals and symbols, each with different meanings.

---

and offered choice.").

[197] *Id.* at 29:41 (statement of Bob Liodice, President of the Ass'n of Nat'l Advertisers) ("It is easy for consumers and it works.").

[198] *Id.* at 30:24, 30:36 (statement of Bob Liodice, President of the Ass'n of Nat'l Advertisers) ("The Icon is . . . served in over one trillion ad impressions each month. . . . More than one million consumer opt outs have been registered under the DAA Principles since January 2011 . . . .").

[199] *Id.* at 34:36 (statement of Alex Fowler, Head of Privacy at Mozilla) ("The ad industry's own research shows the number of users who use the icon is below four hundredths of a percent.").

[200] *See supra* note 198 and accompanying text.

[201] *See Self-Regulation Hearing*, *supra* note 10, at 36:06 (statement of Alex Fowler, Head of Privacy at Mozilla) ("Nine percent of our users have turned on do not track in Firefox and eighteen percent have it on in our mobile browser.").

[202] *See* Ed Bott, *The Do Not Track Standard Has Crossed Into Crazy Territory*, ZDNET.COM (Oct. 9, 2012, 9:42 PM), http://www.zdnet.com/the-do-not-track-standard-has-crossed-into-crazy-territory-7000005502/ (discussing a statement by Microsoft's Chief Privacy Officer, Brendon Lynch).

[203] HODDER ET AL., *supra* note 64.

[204] PURCELL, BRENNER, & RAINIE, *supra* note 64

[205] *Self-Regulation Hearing*, *supra* note 10, at 34:26 (statement of Alex Fowler, Global Privacy and Policy Leader, Mozilla) ("Many believe that clicking on the icon will trigger pop-up ads or invite more advertising, and many more think it's related to purchasing advertising space.").

[206] *See Your AdChoices 101*, DIGITAL ADVERTISING ALLIANCE, *http://www.youradchoices.com/learn.aspx* (last visited July 13, 2013) (instructing how to use the Advertising Options Icon).

¶108 Given that transaction costs are central to the political strategy of limiting consumer choice online, transaction costs should continue to play an increasingly important role in privacy analysis. Too often economic argumentation about privacy is directed toward a costless bargaining world. In such a world, for example, consumers would be able to express their preferences at no cost, and therefore there would be no need for integration or automation.[207] But this is a severely limited view of economics. A better approach might be to say that the concept of the Coasean bargain does not render transaction costs irrelevant, but instead makes transaction costs central to every theory.[208] If bargains are costless, certain results follow. But if bargains are not costless—and here they are not—then those results do not follow. Using transaction-cost-free analysis to describe the market in personal information is like using friction-free physics to describe a football game.

¶109 Preferences in privacy will be better served by reducing transaction costs, than by applying a model of substantive privacy that raises costs. Whichever privacy model one asserts to be true, it can only face a true market test if both consumers and corporations are permitted to use the lowest-cost method of communicating their preferences. In the online context, that lowest-cost method is the use of automated, default, integrated features set by software agents.

IV. CHALLENGES AND ANSWERS

¶110 This section seeks to anticipate and answer counterarguments. The most compelling point against all of the following potential counterarguments is that their effect is to avoid a market test between automated and bespoke privacy features. The following subparts address and evaluate each potential counterargument in turn.

A. Is Tracking Preference Expression Trivial?

¶111 A first potential challenge is that it is trivial to set the flag. The argument runs as follows: The American public does not want privacy. For those rare zealots who do want privacy, it is not too much to ask that they set a Do-Not-Track flag by hand. Their privacy will then be safeguarded and the Internet will continue to be funded by consumer tracking.

¶112 This argument fails because both sides agree that the default rule for privacy significantly influences the contours of the market.[209] This is why the underlying battle between opt-in and opt-out tracking has been so bitterly debated.[210] If the default rule is

---

[207] *See* Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745, 749 (2003) ("Research about the relative costs of opt-in versus opt-out rules would be irrelevant in a world of costless transactions. A Coasian view of bargaining over the rights to use personally identifiable information concludes that if negotiating and contracting is costless, the usage rights will accrue to the party with the greatest value, regardless of the initial assignment.").

[208] *See generally* Coase, *supra* note 62.

[209] *See* Alexei Alexis & Donald G. Aplin, *Online Advertising Coalition Rejects Microsoft Do-Not-Track Browser Default*, BLOOMBERG BNA (Oct. 15, 2012), http://www.bna.com/online-advertising-coalition-n17179870251/ (discussing the issue's importance to and the opinions of the Digital Advertising Alliance, two House of Representatives members, the Federal Trade Commission, and the European Union Commissioner for the Digital Agenda).

[210] *See Angwin*, *supra* note 14 ("Stu Ingis, general counsel of the [Digital Advertising Alliance], called

privacy, most people will not change that default.[211] If the default rule is tracking, most people will not change that default.[212] The selection of default is therefore not trivial.

¶113 The argument that default Do-Not-Track is trivial further rests on the assumption that advertisers would honor the user's tracking preference if it were set by hand. But advertisers do not respect hand-set DNT flags,[213] and the effect of banning default Do-Not-Track is that even more hand-set DNT flags will be ignored. Do-Not-Track flags are now in all major browsers, and vanishingly few advertisers honor them. The flags that are in current major browsers are all bespoke. Users must set them by hand, and few people do. But corporations ignore even those flags that meet the bespoke standard. The fight over default Do-Not-Track serves only to undermine the standard so that corporations may continue to ignore the flags.

¶114 The argument that switching is trivial also relies on individual feature cost, not aggregate cost. The aggregate time cost of configuring privacy controls is not trivial. Consider the protections that a consumer must configure by hand as things currently stand. She must install and configure malware-detecting software to stop computer applications from spying on her. She may want to try Linux. She must find a way to automate encrypted connections to prevent over-the-wire spying from her Internet service provider (ISP). She must find a way to avoid traffic analysis, usually by means of a proxy or VPN. She must disable cookies. She must regularly conduct maintenance to attempt to remove cookies that circumvent her protections.[214] She must install and configure ad-blocking software, since the advertisements that are served track her movements across the web. She must select a search engine, like Ixquick's Startpage.com, that does not track her online searches.[215] She may, at an entirely different level of futility, read and attempt to understand online privacy policies or manage the plethora of ad preferences managers, privacy icons, privacy seals, or other complicated privacy controls offered by online advertisers, ISPs, and website hosts.

¶115 But she is still not done. She must, finally, find and enable the Do-Not-Track flag. Each individual step does not seem difficult, but in the aggregate, the process is prohibitively cumbersome.[216] Even if she takes all these steps, her movements online

---

Microsoft's move a 'unilateral' decision that 'raises a lot of concern.' He said that the industry supports 'consumer choice, not a choice made by one browser or technology vendor.'"); *see also* Shankland, *supra* note 3 ("Roy Fielding, an author of the Do Not Track (DNT) standard and principal scientist at Adobe Systems, wrote a patch for Apache that sets the Web server to disable DNT if the browser reaching it is Internet Explorer 10. 'Apache does not tolerate deliberate abuse of open standards,' Fielding titled the patch."). *But see* Grimmelmann, *supra* note 10 (Written Testimony of James Grimmelmann).

[211] *See* Kesan & Shah, *supra* note 4, at 601 ("If a person does not know about the possibility of changing an option or the ramifications of each choice, then a default setting is equivalent to a fixed setting.").

[212] *See id.*

[213] *See* Martha Neil, *Some Advertisers Say Their Compliance with Computer Browser Do-Not-Track Feature Is Optional*, ABA. J. (Oct. 11, 2012, 12:00 PM), http://www.abajournal.com/news/article/some_advertisers_say_ compliance _with_ computer_browser_do-not-track_feature/.

[214] *See* Soghoian, *supra* note 30 (discussing the process consumers must go through to set and maintain opt out cookies).

[215] *See Privacy Policy*, START PAGE, https://startpage.com/eng/privacy-policy.html#qdata (last updated June 2013) ("*We don't collect any personal information on our visitors.*").

[216] *See* Richmond, *supra* note 140 ("Keeping your computer free of tracking programs is not easy because of the ad industry's aggressive and sophisticated efforts . . . . A number of tools can minimize tracking, but using them requires considerable effort and tech know-how.").

possess only a bare modicum of privacy, easily breached by anyone willing to step even the slightest bit outside of the rules. A better option is to simply download a browser that contains these features as an integrated, automated, and optimized feature set.[217] It is precisely this option that the TPE bespoke standard forecloses.

¶116 There is only one solution to the problem of aggregate costs of privacy protection. Privacy features must multiply as tracking techniques multiply. Just as tracking techniques must be automated to be effective, so must privacy features be part of a comprehensive, integrated, and automated consumer package in order for the consumer to get any practical protection at all. The contrary view, that additional tracking techniques may be implemented automatically, while any additional privacy features must be enabled by hand, simply imposes imbalanced transaction costs on consumers. If tracking can be automated while privacy features must be enabled by hand, few additional privacy features will be added to products, and almost none will be enabled.

B. Does Default Do-Not-Track Muddy the Standard?

¶117 A second claim is that default Do-Not-Track blurs the communicative power of the DNT flag. The argument is that Do-Not-Track is powerful because it stands for the consumer's expressed preference not to be tracked.[218] Permitting software to configure that preference, goes the claim, muddies the standard because the corporation now cannot be sure that the consumer truly wished not to be tracked.[219]

¶118 Advertisers have long attempted to argue that they could not be held responsible for respecting any Do-Not-Track flag because the meaning of the flag was unclear.[220] Yet the presence of an obvious, continuous machine-readable Do-Not-Track flag is not merely clear, it is unavoidably clear. The problem is not that corporations do not understand what a Do-Not-Track flag means, it is that they wish to manufacture doubt as to how the flag was set so that they may continue to track.[221]

---

[217] *See* Ohm, *supra* note 51.

[218] *See* Roy Fielding, Comment to *Apache Does Not Tolerate Deliberate Abuse of Open Standards*, GITHUB, https://github.com/apache/httpd/commit/a381ff35fa4d50a5f7b9f64300dfd98859dee8d0#commitcomment-1819635 (last visited Oct. 18, 2012) ("The only reason DNT exists is to express a non-default option. That's all it does. It does not protect anyone's privacy unless the recipients believe it was set by a real human being, with a real preference for privacy over personalization.").

[219] *See* E-mail from Mike Zaneis to David Singer, *supra* note 175 ("If the site does not believe the DNT:1 signal is valid, then why would anyone in the supply chain be expected to honor the invalid signal?").

[220] *See* Elise Ackerman, *Google and Facebook Ignore "Do Not Track" Requests, Claim They Confuse Customers*, FORBES (Feb. 27, 2013, 7:58 PM), http://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/ (" [S]pokespeople from Google and Facebook explained that they are not responding to "do not track" requests because it isn't clear that consumers know what "do not track" means. Keith Enright, a senior policy counsel at Google, said there is a "consumer confusion question" that is caused by the fact that there is still no official, industry-accepted "Do Not Track" standard. Acknowledging a consumer's "do not track" preference "in some ad hoc way" may not be meeting that user's expectations, Enright explained. Erin Egan, the chief privacy officer of Facebook, said she also wasn't sure that a "do not track" setting on a browser actually reflected a user's desire not to be tracked, especially in cases where a company like Facebook was tracking users in order to customize their web experience, rather than to sell advertising.").

[221] *Cf.* Ohm, *supra* note 51.

¶119 The attack on default Do-Not-Track is useful to advertisers precisely because it will spill over and permit advertisers to ignore all Do-Not-Track flags, bespoke, or default. If a user sets the flag, that flag is set to DNT:1.[222] If the browser sets the flag during the customer's installation process, the flag is also set to DNT:1. The only way that a web server can determine whether the flag was set by default or by hand is to query the browser, termed "user agent sniffing" or "browser sniffing," which is considered bad coding practice.[223] But even this technique will not work in the long run, since the web server can only sniff information that the browser conveys. If the browser conveys only the information that the flag has been set DNT:1, the web server cannot distinguish.

¶120 The only long-term way to stop automated Do-Not-Track is to target specific companies and products that offer it. In the case of Microsoft's IE10, web servers must be programmed to ignore all Do-Not-Track flags set by IE10.[224] Only an overall attack on the entire DNT standard will work. And this overall attack coincidentally happens to invalidate hand-set DNT flags in one of the world's most popular lines of browsers. The attack on default Do-Not-Track is an unsubtle attack on all of Do-Not-Track, since there is no way to tell whether the flag was set by hand, by default, or during the installation process. Unfortunately, this attack stands a good chance of succeeding, given the current adoption of the bespoke standard in the TPE.

¶121 A good example of an attack on DNT was the 2012 patch released for Apache, the web server software that runs a good portion of corporate-side websites. The proposed patch ignored the Do-Not-Track flag on the ground that it has not been set by the consumer.[225] This approach has a certain tit-for-tat appeal. After all, if consumers can automatically set Do-Not-Track flags, perhaps corporations can automatically ignore them. The patch was eventually commented out by the Apache community,[226] but the point it made was clear: developers who protect privacy by enabling Do-Not-Track by default run the risk of losing privacy protection for all of their customers, including those who set the flag by hand.

¶122 Simply ignoring DNT flags on a browser level also ignores the underlying apparatus of contract law. If a corporation receives clear, unambiguous notice that a consumer does not consent to tracking, the corporation should not be permitted to proceed with the transaction as if that preference were not communicated. A brief example may clarify. Imagine the following scenario: I go into a store and offer to buy a $100 television set for $25. The store has the right to set whatever price it wishes, without a doubt. It has the power to refuse to sell to me for $25. But it absolutely does not have the right to accept my offer, sell me the TV, and then charge my credit card $100.

---

[222] *See W3C TPE Draft*, *supra* note 5, § 6.3.1 (discussing guidelines for interaction with existing user privacy controls).

[223] *See Browser detection using the user agent*, MOZILLA DEVELOPER NETWORK, https://developer.mozilla.org/en-US/docs/Browser_detection_using_the_user_agent (last visited August 8, 2013) ("Important: It's worth re-iterating: it's very rarely a good idea to use user agent sniffing.").

[224] *See, e.g.*, Shankland, *supra* note 3 ("As a result of the Apache update, Web servers using the software will ignore DNT settings for people using IE10.").

[225] *Id.*

[226] *See* Jonathan Mayer, Comment to *Bug 53845 - Remove DNT Settings From httpd.conf*, THE APACHE SOFTWARE FOUNDATION (Oct. 9, 2012, 2:40 AM UTC), https://issues.apache.org/bugzilla/show_bug.cgi?id=53845 ("The configuration lines for Do Not Track in Internet Explorer 10 have been commented out.").

¶123 In the DNT context, a company may exclude the consumer from its website if a consumer's tracking preference kills the deal. Or the corporation may propose a counteroffer. This is how some sites handle cookies now. The user is excluded until they enable cookies. The corporation may thus refuse the consumer's terms, or rewrite the terms of its own contract to offer a different deal. But the corporation may not rewrite the terms of the consumer's offer.

¶124 A threat to ignore all DNT flags set by a given browser is a threat to any company that proposes an advance in automatic, default privacy protections for consumers. If IE10 chooses to enact positive privacy protections for its users, online advertisers will deny IE10 users privacy protections that they extend to other browser users. The very attribute that might make IE10 attractive to consumers (that it takes privacy protections seriously, at least in this respect) is directly undermined—indeed destroyed—by the threat of online advertisers to retaliate against consumers who choose IE10.

¶125 For this reason, it is important to think about consumer choice as being exercised at the product level and not merely at the feature level. Whereas corporations claim they are forced to ignore DNT flags because they have too little information, they are in fact ignoring the Do-Not-Track flag precisely because they have a glut of information. When a corporation receives a Do-Not-Track flag from an IE10 browser, the corporation is acting not only upon knowledge of receipt of the browser flag, but also on knowledge of the browser installation process and feature set.

¶126 In acting from a surfeit, rather than a lack, of knowledge, advertisers have done significant damage to the credibility of their claim that default Do-Not-Track is unclear. The corporation has received a request not to track. In fact, the corporation knows that the browser the consumer chose has Do-Not-Track as a core feature of the product. Now the corporation has the unenviable position of explaining why it wishes to ignore the flag.

¶127 Moreover, suppose this standard for signal clarity were turned on corporations. Suppose that corporate contracts were not enforceable if the consumer could manufacture some doubt as to whether the corporation really wanted the term, as opposed to merely including it in automated boilerplate. This cannot be the online standard for contract formation. Online parties are bound by the contract terms their software agents express.

¶128 The inconsistency runs deeper. Corporations are not so solicitous of the absolute agreement of consumers to every online term. Usually consumers are bound by terms they have not even reviewed.[227] Yet under the corporate analysis, a Do-Not-Track term is different. The consumer must express this particular term—the Do-Not-Track term—by hand precisely because the advertising companies do not want the term to be expressed.

C. Can Corporations Undo Do-Not-Track with EULAs or Terms of Service?

¶129 The TPE implies in its discussion of Tracking Status Value that even if a consumer sends a valid, non-default DNT flag, a web server may still ignore that flag, based on the web server operator's belief that the server has received separate consent to tracking.[228] The W3C's Tracking Compliance and Scope document expressly permits out-of-band

[227] *See* James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 YALE J. INT'L L. 109, 120–21 (2003) ("[C]onsumers do not read standard terms . . . .").

[228] *See W3C TPE Draft*, *supra* note 5, § 6 (discussing principles that "guide the design of user-agent-managed exceptions").

consent to trump the DNT signal.[229] This creates a loophole that could potentially swallow the rule, since out-of-band consent is not limited in time, nor can consent be retracted through the DNT process. Note, also, that the question is framed expressly in terms of the corporation's belief that it has received prior consent. The ability to ignore the DNT flag is based on the designated resource's "belie[f] it has received prior consent for tracking this user, user agent, or device, perhaps via some mechanism not defined by this specification, and that prior consent overrides the tracking preference expressed by this protocol."[230]

¶130 Out-of-band consent creates a real problem for Do-Not-Track, especially when the licensor of an internet access device is the same as the licensor of the internet browser the consumer uses. If the Apple iPad license purports to exempt Apple services and affiliates from Do-Not-Track, or if the Android license exempts Google from Do-Not-Track, the standard will be unlikely to meet consumer expectations of privacy. All Android users would be vulnerable to tracking across nearly half of the internet. What the company gives in the browser, it takes away in the device licenses. And this is very likely to happen: many believe the primary reason that Google licenses Android for free is because the device then privileges Google's search and advertising functions for users of the device.[231] The upshot is that out-of-band consent will serve mostly as a way of tricking consumers who believe their DNT flag will be respected.

¶131 There is some hope that default automated browser responses might be able to limit this otherwise gaping loophole. The Tracking Status Value section of the TPE does state, at the least, that servers that believe they are relying on prior consent must, for example, indicate that prior consent by returning a Tracking Status Value of "C" to the user's transmission of the DNT:1 flag.[232] This might permit browser manufacturers to build in options that permit users to reject "C" Tracking Status Values. But this would require either the browser to set the "C" rejection automatically (raising the question of automation and defaults all over again), or would require the consumer to understand and configure the browser to deal with an additional level of complexity. This creates a vicious cycle of complexity, increasing consumer costs again, even if it were to work.

D. Will Respecting Consumer Privacy Damage the Internet?

¶132 Another often-repeated argument raised by industry advocates is that targeted advertising is the only method of monetizing the Internet that has thus far worked.[233]

---

[229] *See Tracking Compliance and Scope*, *supra* note 102, § 6.3.

[230] *See W3C TPE Draft*, *supra* note 5, § 5.2.6.

[231] *See* Steven Musil, *Google Now Facing Antitrust Scrutiny in Europe over Android*, CNET (Apr. 8, 2013, 4:11 PM), http://news.cnet.com/8301-1023_3-57578545-93/google-now-facing-antitrust-scrutiny-in-europe-over-android/ ("Google is facing a fresh round of antitrust scrutiny from the European Union, this time for Android. The revelation emerges as the Web giant tries to resolve EU charges related to how it displays search results, which critics say favor the company's own services over those of its competitors.").

[232] *Id*.

[233] *See* Holman W. Jenkins Jr., *Google and the Search for the Future*, WALL ST. J, Aug. 14, 2010, http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html?mod=WSJ_Opinion_LEADTop (discussing an interview with Eric Schmidt, Google's CEO: "[T]he only way I know of to increase monetization is through targeted ads. That's our business."); *see also* Bott, *supra* note 202 (providing an additional view on the value of advertising, advocated by a member of the W3C working group: "Marketing fuels the world. It is as American as apple pie and delivers relevant advertising to consumers about products they will be interested at a time they are interested. DNT should permit it as one

Respecting consumer preferences regarding privacy would kill this model, they claim.[234] They assert that the effect would be particularly strong if the default rule for tracking were changed by default Do-Not-Track. This would create a de-facto "opt-in" system for tracking. The large majority of consumers would not opt in, goes the logic, and thus online targeted advertising would suffer.

¶133 This argument seems quite correct. Indeed, it is tautological. Prohibiting invasions of privacy will inhibit business models based on invading privacy. Reducing transaction costs for consumers to defend their privacy will sit poorly with corporations who have enjoyed untrammeled access to consumer data.[235] While the argument is correct, it does not help us decide between benefits to corporations and costs to consumers.

¶134 Industry is never pleased with rules that prevent forcing deals or ads on consumers without their consent. The publishing industry was undoubtedly displeased with rules saying that they could not ship products to people without consent and then charge them.[236] The advertising-by-fax industry was certainly displeased by the TCPA's ban on unsolicited fax advertising.[237] The telemarketing industry was certainly not pleased with the federal Do-Not-Call list.[238] The bottom line is the same: Banning coercive sales and invasive advertising practices harms industry, but the overall harm to society of permitting these kinds of techniques is greater.[239]

¶135 The relevant question is not whether corporations will be better or worse off if consumers can protect their privacy. A better question would include costs and benefits to consumers as well as to industry. The best question would be whether the benefit to consumers of privacy, as measured by the market, outweighs or is outweighed by the benefit to consumers of services that are financed through datamining personal information. The best way—perhaps the only way—to ask this question is to permit a

---

of the most important values of civil society. Its byproduct also furthers democracy, free speech, and—most importantly in these times—JOBS. It is as critical to society—and the economy—as fraud prevention and IP protection and should be treated the same way.")

[234] *See* Jim Puzzanghera, *Do-Not-Track Bill Worries Some Lawmakers*, L.A. TIMES, Dec. 3, 2010, http://articles.latimes.com/2010/dec/03/business/la-fi-do-not-track-20101203 ("Requiring a do-not-track mechanism to protect consumers from companies tracking their digital footprints on the Web . . . could damage the Internet economy.").

[235] *See* Hayley Tsukayama, *Pandora IPO Echoes Larger Anxieties over Do Not Track*, WASH. POST, Feb. 18, 2011, http://voices.washingtonpost.com/posttech/2011/02/pandora_ipo_reveals_concerns_a.html (discussing an interview with Jeffrey Chester of the Center for Digital Democracy: "'They're spending billions of dollars on a ubiquitous data collection system, only to find it might be thrown in the digital junk heap,' if Do Not Track is approved").

[236] *See* 39 U.S.C. § 3009 (a)–(b) (2006) ("[T]he mailing of unordered merchandise . . . constitutes an unfair method of competition and an unfair trade practice . . . . Any merchandise mailed in violation of subsection (a) of this section . . . may be treated as a gift by the recipient . . . .").

[237] *See* Missouri ex rel. Nixon v. Am. Blast Fax, Inc., 323 F.3d 649, 652 (8th Cir. 2003) ("The fax companies . . . argu[ed] that § 227(b)(1)(C) was an unconstitutional restriction on their freedom of speech.").

[238] *See* Mainstream Mktg. Servs., Inc. v. F.T.C., 358 F.3d 1228, 1246 (10th Cir. 2004) ("The telemarketers . . . challenge[d] various . . . aspects of the do-not-call registry[:] . . . 1) whether the fees telemarketers must pay to access the registry are constitutional, 2) whether it was arbitrary and capricious for the FCC to approve the established business relationship exception, and 3) whether the FTC had statutory authority to enact its do-not-call rules.").

[239] *See, e.g.*, Cheryl Tucker, *$50,000 Well Spent: Blocking Robocalls*, THE NEWS TRIBUNE (Oct. 19 2012, 6:30 AM), http://blog.thenewstribune.com/opinion/2012/10/19/50000-well-spent-blocking-robocalls/ (discussing how automated calls "bombard[] people in a struggling economy with promises of debt assistance and cheap loans").

true market test. Browsers with automated and default privacy functionality must be permitted to compete with browsers that require users to configure privacy features by hand. Insisting that consumer preferences can only be honored in one or the other fashion intentionally distorts the market test.

¶136 Industry claims of harm due to competition should also be taken with a grain of salt.[240] Microsoft is no privacy angel.[241] Microsoft is trying to make money by providing enhanced privacy features. It has determined through focus groups that setting Do-Not-Track as a default resonated with potential customers. Microsoft is trying to make a profit by making its products more competitive with respect to the ease of privacy protection configuration.

¶137 The addition of default Do-Not-Track is not a story of market failure. It could be a story of successful competition to add privacy features. However, at the moment it is a story about the anticompetitive attempt to keep such products out of consumers' hands, or to ensure that they go largely unused. As Microsoft's own checkered antitrust history shows, companies may well complain of harm when they are outcompeted.[242] Yet social welfare is maximized by a free and open market. Industry advocates want to undermine a key feature of a competing product. But competition helps society. The arguments from industry harm make it clearer than ever that corporate and social welfare are simply not identical, and are in cases of anti-competitive behavior directly opposed.

V. CONCLUSION

¶138 The discourse over Do-Not-Track seems to have achieved broad consensus that some form of the technology will be implemented. But there is a devil in the details. Many prior privacy initiatives have failed due to the lack of usability and consumer exhaustion. A solution must be as simple as technology can make it, for it to have any chance of success. Advertisers are willing to see the Do-Not-Track standard fail rather than permit it to be low-cost enough for the majority of consumers to use. Their

---

[240] *See* Will Oremus, *Google Grudgingly Adds "Do Not Track" Privacy Option to Chrome Browser*, SLATE (Sept. 14, 2012, 6:07 PM), http://www.slate.com/blogs/future_tense/2012/09/14/google_do_not_track_chrome_browser_adds_support_for_online_privacy_setting_.html ("Google recognizes that Do Not Track is far from the worst-case scenario. For one thing, it's better for Google than watching Chrome users flee for the shelter of Mozilla or Apple, let alone Microsoft."); *see also* Scott Meyer, *The Real Impact of Do Not Track*, AD AGE (Oct. 17, 2012), http://adage.com/article/digitalnext/real-impact-track/237808/ ("If DNT is implemented the way that Microsoft, some regulators and hard-core privacy advocates want, the big winners are—wait for it—the biggest American internet companies with their huge first-party opt-in databases.").

[241] *See* Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the* Government, 12 MINN. J.L. SCI. & TECH. 191, 194 (2011) ("Microsoft has pledged that it takes its 'customers' privacy seriously. However, when asked by the New York Times if the company was considering a policy to log no search data at all, Peter Cullen, Microsoft's chief privacy strategist, argued that too much privacy was actually dangerous."); *see also* Edward Wyatt & Nick Wingfield, *As Microsoft Shifts its Privacy Rules, an Uproar is Absent*, N.Y. TIMES, Oct. 19, 2012, http://www.nytimes.com/2012/10/20/technology/microsoft-expands-gathering-and-use-of-data-from-web-products.html?pagewanted=all&_r=0 ("Microsoft instituted a policy on Friday that gives the company broad leeway over how it gathers and uses personal information from consumers of its free, Web-based products like e-mail, search and instant messaging.").

[242] *See* Diane Bartz, *Microsoft vs US Antitrust Battle Soon to be History*, REUTERS (Apr. 27, 2011, 6:29 PM), http://www.reuters.com/article/2011/04/27/microsoft-antitrust-idUSN2718770120110427 (discussing antitrust lawsuit against Microsoft that spanned thirteen years).

opposition to default Do-Not-Track may very well succeed in disrupting Do-Not-Track as a whole.[243]

¶139 The attack comes not directly against Do-Not-Track, but through the requirement that the Do-Not-Track flag be set by hand. The theoretical underpinning of the attack comes in the form of an argument about online consent. According to the standard, consumers may not express their preference against tracking at the product level by preferring pro-privacy products. They may only consent at the feature level, by finding and hand-configuring privacy features. Yet only product-level consent, not feature-level consent, will permit consumers to defend their privacy.

¶140 Requiring users to enable privacy features by hand does not ensure consent, since it excludes those consumers who express consent at the product level by buying and using pro-privacy products. The bespoke standard merely raises transaction costs. These transaction costs cause a huge shift in whether the privacy tool is used or not. Further, the bespoke standard creates a double standard in favor of corporations and against consumers. It makes as much sense to require consumers to set their privacy preferences by hand as it does to require corporations to conduct their online tracking by hand. Corporations do all of their online contracting through automated agents, but wish to require consumers to protect their privacy preferences by hand.

¶141 Finally, the bespoke standard is profoundly anticompetitive. A refrain from industry advocates throughout the congressional hearings on Do-Not-Track is that they passionately believe that companies will respond to the demand for privacy by introducing products with better privacy features.[244] A company has done so, and the response from the standard-setting group and advertising industry has been to undermine the efficacy of that feature and punish all consumers who use the pro-privacy product. This is not the behavior of a healthy market in privacy features for consumers.

¶142 The opposition from advertising industry advocates is an attempt not to clarify what was unclear, but to complicate the simple. The bespoke standard of the TPE is a step in the wrong direction. It should not become a standard; it should not be adopted as best practices by the FTC; and it certainly should not find its way into any developing legislation. For Do-Not-Track to be effective, it must be capable of being delivered to

---

[243] *See* Juliana Gruenwald, *Do-Not-Track Proposal Headed Off the Tracks*, NAT'L JOURNAL, http://www.nationaljournal.com/tech/do-not-track-proposal-headed-off-the-tracks-20121009 (last updated Oct. 9, 2012, 4:16 PM) ("'DAA is trying to turn DNT into TNT and blow the process up,' said Jeff Chester, executive director for the Center for Digital Democracy. . . . Electronic Frontier Foundation Staff Technologist Dan Auerbach also . . . said 'it seems clear they [advertising industry officials] want to stifle the progress' on do-not-track." (alteration in original)).

[244] *See Self-Regulation Hearing*, *supra* note 10 (testimony of Bob Liodice, President and Chief Executive Office Association of National Advertisers, Inc.) ("Companies are increasingly offering consumers new privacy features and tools such as sophisticated preference managers, persistent opt outs, universal choice mechanisms, and shortened data retention policies. These developments demonstrate that companies are responsive to consumers and that companies are focusing on privacy as a means to distinguish themselves in the marketplace."); *A Status Update on the Development of Voluntary Do-Not-Track Standards: Hearing Before S. Comm. On Commerce, Science, and Transportation*, 112th Cong. 17 (2013) (written Testimony of Luigi Mastria, Managing Director, Digital Advertising Alliance), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=cd2e39e0-6825-4b8c-9789-40d26a72d457 ("[L]egislation thwarts innovation and hinders economic growth and can impede a competitive marketplace that offers a full range of choice to consumers.").

and used by consumers like any other software tool. Advertisers are attempting to confuse what is already very clear. Do-Not-Track means do not track.