KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

**Statement of Justin Brookman**
Director, Consumer Privacy
Center for Democracy & Technology

**Before the U.S. Senate Committee on Commerce, Science, and Transportation**

*Hearing on*
"A Status Update on the Development of Voluntary Do-Not-Track Standards"

April 24, 2013

Chairman Rockefeller, Ranking Member Thune, and Members of the Committee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the leadership the Chairman has demonstrated in examining the challenges in developing a consensus Do Not Track standard and appreciate the opportunity to address the continued insufficiency of self-regulatory consumer privacy protections.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. I currently serve as the Director of CDT's Consumer Privacy Project. I am also an active participant in the Worldwide Web Consortium's Tracking Protection Working Group, where I serve as editor of the "Tracking Compliance and Scope" specification — the document that purports to define what Do Not Track should mean.

My testimony today will briefly describe the history of online behavioral advertising and the genesis of the Do Not Track initiative. I will then describe the current state of the World Wide Web Consortium's efforts to create Do Not Track standards and the challenges going forward to implement Do Not Track tools successfully. I will conclude with my thoughts on the future of Do Not Track. and why I believe that this protracted struggle demonstrates the need for the fundamental reform of our nation's privacy protection framework for commercial and government collection and use of personal information.

**The Rise of Behavioral Advertising**

Online behavioral advertising has been a concern for regulators and privacy advocates for over fifteen years now. Behavioral advertising, or more specifically *cross*-site behavioral advertising, was originally made possible because of two core capabilities afforded by web browsers: cookies and referer headers. Cookies are small bits of code that the operator of a website can store locally on

a user's computer — among other things, they can be used as unique IDs so that a website can recognize a particular user (or device) when the user returns to a particular website. Originally conceived as a means for first-party services to keep remember a user over time, soon advertising networks — the companies that websites often use to generate ads for them — began to place unique cookies' on web users' browsers as well. Because web browsers typically identify the referring site when it passes along a web request (the "referer header"), advertising networks were informed of the precise webpage they served a user a particular advertisement. Combining cookies and referer headers together, advertising networks were able to generate detailed logs of the various websites they encountered a particular user.

Eventually, these companies began analyzing this web history to help inform decisions about which ads to show particular users. When an advertiser has a presence on many sites a user may visit, it is able to develop a trail of past web surfing behavior consisting of a list of many individual actions a user has taken online. These trails are very unique in the sense that no two people do exactly the same things online, so advertisers are able to leverage this very rich, unique view of each user to make split-second decisions about what ads to show them that they will have the highest likelihood of noticing and interacting with. In a nutshell, that's what behavioral advertising is — utilizing information about previous sites visited by a particular user to influence decisions about what ads to show in the future.

As the behavioral advertising industry took off, many privacy advocates complained that users did not understand that their cross-site behavior was being tracked by companies they had never heard of, and urged that users should have to affirmatively consent to the tracking of their web surfing habits. In 2000, a class action suit was filed against DoubleClick, a leading behavioral advertising company, arguing that the company's tracking users without consent across websites violated the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. At the same time, the Federal Trade Commission investigated DoubleClick's behavioral advertising practices, and the allegations that DoubleClick intended to attach real names to behavioral profiles. Eventually, the *DoubleClick* lawsuit was dismissed,[1] and the FTC discontinued its investigation of the company, declining to allege that the company's tracking of users without explicit consent violated existing law.[2]

However, while advocates' call for *opt-in* consent for behavioral tracking went unheeded, industry has always acknowledged that users should at least have the right to *opt out* of behavioral advertising.[3] Moreover, for years, there has been general recognition that there must to be a *global* way to opt out of *all* behavioral tracking at once — users cannot reasonably be expected to locate all potential tracking companies and one-by-one opt out of their tracking. Thus, already today, the Digital Advertising Alliance (DAA) — the umbrella self-regulatory group consisting of the Interactive Advertising Bureau, Network Advertising Initiative, Better Business Bureau and others — maintains a site through which users can globally opt out of behavioral advertising by its member companies.[4]

---

[1] *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[2] Letter from the Federal Trade Commission to Christine Varney, January 22, 2001, Re: DoubleClick, Inc., http://www.ftc.gov/os/closings/staff/doubleclick.pdf.

[3] FTC Staff Report, Public Workshop on Consumer Privacy on the Global Information Infrastructure, December 1996, http://www.ftc.gov/reports/privacy/Privacy1.shtm, at II.C.2 (Consumer Choice).

[4] Digital Advertising Alliance, http://www.aboutads.info/choices/.

Unfortunately, there are several limitations to industry's current opt-out structure:

- It only applies to advertisers that are members of the DAA; companies that don't sign up and pay for membership are not included, and receive no indication that a user does not want to be tracked.

- The opt-out is almost always cookie-based. If a user deletes her cookies — or if they are routinely deleted by her anti-virus software, as is often the case — the opt-out disappears, and companies subsequently have no way of knowing that the user does not want to be tracked.

- The opt-out only prevents users from seeing targeted ads, which are based on information gathered from tracking. However, it does not prevent tracking itself. While the DAA's Multi Site Principles in principle agree with the notion of collection limitation, in practice, the code's bases for collection are extremely broad, and any justification to understand "consumer preferences and behaviors [or] research about consumers, products, or services" could justify individualized data collection despite the user's opting out.[5]

- The interface through which users are presented their choices around tracking and opting out both through the AdChoices icon and on the DAA website are confusing.[6]

Coupled with the limitations of the industry's opt-out approach, industry self-regulation has failed to grapple with the dramatic expansion of the scope of tracking online. Websites that used to embed one or two tracking cookies now embed dozens. A *Wall Street Journal* report found that the top 50 websites placed over 3,000 tracking files on a test computer; IAC Interactive's Dictionary.com alone placed 223 tracking files from a variety of third-party companies.[7] In the past year alone, the number of web tracking tags on websites has gone up 53%, nearly half of which were embedded not by the first-party publisher, but by ad networks embedding their own tags to transmit data to still other companies.[8] Moreover, tracking that used to be pseudonymous (profiles tied to a device, but not a name) are increasingly linked or easily linkable to real world identities.[9] Last December, for example, the *Wall Street Journal* reported on a company named Dataium that tracked users by email address, and sent descriptions of

---

[5] Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[6] A. M. McDonald and Lorrie Faith Cranor, *Social Science Research Network*, "Beliefs and behaviors: Internet users' understanding of behavioral advertising," October 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092; Pedro G. Leon et al., *Carnegie Mellon University CyLab,* "Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising," October 2011, http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.

[7] Julia Angwin, "The Web's New Gold Mine: Your Secrets," *The Wall Street Journal*, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[8] George Simpson, "Suicide by Cookies," *MediaPost*, February 22, 2013, http://www.mediapost.com/publications/article/194073/suicide-by-cookies.html#axzz2REncGaSy.

[9] Justin Brookman, CDT blog, "Why Facebook Apps Story is Problem for Entire Web," October 19, 2010, https://www.cdt.org/blogs/justin-brookman/why-facebook-apps-story-problem-entire-web.

online surfing to offline companies with which users had shared that same email address.[10] Industry trade associations have failed to adapt to address new business models predicated on expanded and more personal tracking. As one long-time industry player summarized recently: "Self-regulation hasn't worked the way we promised Washington it would."[11]

**The Call for Do Not Track**

Given the longstanding inadequacy of industry self-regulatory control options, in October 2007, CDT and other consumer advocacy organizations called on the Federal Trade Commission to create a Do Not Track list, similar to the successful "Do Not Call" list that allows users to opt out of telemarketing. Under the original formulation for Do Not Track, online advertisers would have to self-identify to the FTC, which would then compile a list of their domains that track consumers. Browsers that supported Do Not Track would then block any third-party communications to domains on the FTC's block list.[12] Only ad networks that did not use unique identifiers to track users around the web would be able to serve advertisements. As a result, users who turned on Do Not Track would simply see ads that were not specialized for them, since advertisers would not have access to the consumers' recent history on the Web to surmise their interests.[13]

Initially, advocates' call for Do Not Track functionality went nowhere. In July of 2009, researcher Christopher Soghoian and Mozilla privacy engineer Sid Stamm created a prototype add-on for Firefox, which reformulated Do Not Track as a persistent HTTP header appended to all web requests. This would give consumers the option of sending out a digital signal each time the user visits a website, asking companies to stop tracking them from site to site. The Do Not Track header was in many ways an improvement over the original concept, as it did not rely on tracker self-identification, and did not require a centrally-hosted list of tracking domains. However, this approach was offered initially as a proof-of-concept, and was not implemented into the Mozilla Firefox browser.[14]

In July 2010, then-FTC Chairman Jon Leibowitz testifying before this Committee effectively resurrected the idea of Do Not Track, and called upon browser makers and ad networks to work together to implement this technology.[15] The FTC formally recommended the development of

---

[10] Jennifer Valentino-Devries and Jeremy Singer-Vine, "They Know What You're Shopping For," *Wall Street Journal*, December 7, 2012, http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html.

[11] George Simpson, "Suicide by Cookies," *MediaPost*, February 22, 2013, http://www.mediapost.com/publications/article/194073/suicide-by-cookies.html#axzz2REncGaSy.

[12] *Tech Law Journal*, "CDT Proposes That FTC Create a Do Not Track List for Consumer Internet Use," October 31, 2007, http://www.techlawjournal.com/topstories/2007/20071031.asp.

[13] Louise Story, *The New York Times*, "Consumer Advocates Seek a 'Do-Not-Track' List," October 31, 2007, http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html?_r=0.

[14] Emil Protalinski, *The Next Web*, "Everything you need to know about Do Not Track: Mozilla vs Google & Microsoft," November 25, 2012, http://thenextweb.com/apps/2012/11/25/everything-you-need-to-know-about-do-not-track-currently-featuring-microsoft-vs-google-and-mozilla/.

[15] Jeffrey S. Edelstein and Linda A. Goldstein, *Lexology,* "Privacy Update: Senate bill and FTC "Do-Not-Track list?" August 12, 2010, http://www.lexology.com/library/detail.aspx?g=5cf00693-fda7-4d91-a1b1-61a70f795565.

Do Not Track in its 2010 draft privacy report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.[16]

In response to Chairman Leibowitz's call, browser makers moved surprisingly quickly to offer Do Not Track features. One week after the draft report was released, Microsoft announced that Internet Explorer 9 would include Tracking Protection Lists, which give consumers the option to block communications to all third-party domains listed on a specific blacklist.[17] This approach mirrored the advocates' original 2007 conception of Do Not Track, which was predicated on blocking tracking domains. However, rather than rely on a centralized list of trackers, Microsoft encouraged others to create and publish their own list of trackers for users to download.

The next month, Mozilla announced it would implement the header approach to Do Not Track in its Firefox web browser, allowing users to send out a persistent header to all websites indicated a preference not to be tracked. Quickly, popular support within the privacy community coalesced around the notion that the header approach was the most viable way to implement Do Not Track, and within several months, all the major browsers offered users a means to append Do Not Track headers to all web requests.[18]

Perhaps most significantly, in February of 2012, at a White House event to announce President Obama's proposed comprehensive privacy protection framework, the DAA announced that it would begin work to allow users to opt out of behavioral advertising using browser based headers. At the time, the DAA stated that it would enforce its self-regulatory choice principles when a user had been provided information about "the effect of exercising such a choice," and when the user had affirmatively chosen to exercise her choice using the browser based header.[19] The DAA stated in February of 2012, "The DAA is committed to making such choices work for all consumers. . . . The DAA expects that such functionality will be implemented within nine months."[20]

---

[16] Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. This call was repeated in the final version of the report issued 16 months later. Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, March 2012, http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[17] Josh Lowensohn, *CNET*, "Internet Explorer 9 to get tracking protection," December 7, 2010, http://news.cnet.com/8301-10805_3-20024864-75.html.

[18] *Crowd Science*, "A Brief History of Do Not Track (DNT)," August 2012, http://www.crowdscience.com/2012/08/a-brief-history-of-do-not-track-dnt/#!prettyPhoto.

[19] Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism*, http://www.aboutads.info/resource/download/DAA_Commitment.pdf.

[20] *Id.*

**Status of Do Not Track Today**

However, despite industry's commitment from 14 months ago, today, only a handful of third-party companies acknowledge and respond to Do Not Track headers in any way.[21]

For some time, the delay in implementation was perhaps justified by a lack of agreement on what exactly the Do Not Track signal should mean. Much of this debate has taken place within the Tracking Protection Working Group of the World Wide Web Consortium (W3C). W3C is a voluntary web standards setting body made up of industry members, privacy advocates, and academic experts; historically they have promulgated standards for the Web on a wide range of matters, such as Web Design and Applications, Web Architecture, and the Semantic Web.[22] The Tracking Protection Working Group was established originally in response to Microsoft's request to standardize Tracking Protection Lists, but was subsequently chartered to form a standard for a universal Do Not Track request tool.[23]

However, this delay has become less defensible over time as the Tracking Protection Working Group has failed to come to consensus on a number of key issues. For well over a year now, the group has effectively stalled on how to address:

- *Cookies*: Privacy advocates have argued that parties honoring Do Not Track should be prohibited from using cookies or other unique identifiers, which would allow those companies to more easily recognize users across websites. In response, industry has argued that cookies should be available for limited purposes (such as fraud prevention or ad frequency capping). This has been a point of contention within the group from the beginning, and indeed back to the original call for Do Not Track in 2007.[24]

- *Market research and product improvement:* Apart from the question of *what* data can be collected despite a Do Not Track signals is the question of *why* data may be collected and retained despite a Do Not Track signal. All parties within the working group are generally in agreement that some data may be collected for basic operational purposes, such as ad delivery, security, frequency capping, and accounting. However, some working group participants have sought to allow the

---

[21] Do Not Track, http://donottrack.us/implementations; Yahoo! Policy Blog, Shane Wiley, *Yahoo! Launches Global Support for Do Not Track*, March 29, 2012, http://www.ypolicyblog.com/policyblog/2012/03/29/yahoo-launches-global-support-for-do-not-track/. However, the ways in which these companies honor Do Not Track is not standardized and varies considerably. Moreover, not all Do Not Track headers are acknowledged: industry trade associations have excused members from adhering to Do Not Track instructions from Microsoft Internet Explorer 10 due to disagreement over whether those implementations reflect user choice. Katy Bachman, "Take That, Microsoft: Digital Ad Community's Final Word on Default Do Not Track," *Ad Week*, October 9, 2012, http://www.adweek.com/news/technology/take-microsoft-digital-ad-communitys-final-word-default-do-not-track-144322.

[22] W3C, Standards, http://www.w3.org/standards.

[23] W3C, Tracking Protection Working Group, http://www.w3.org/2011/tracking-protection/.

[24] W3C Tracking Protection Working Group, Tracking Compliance and Scope, No Persistent Identifers, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#no-persistent-identifiers; CDT, "Consumer Rights and Protections in the Behavioral Advertising Sector," October 31, 2007, https://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

collection and use of data for broader purposes such as market research and product improvement. These purposes are certainly legitimate and societally worthwhile, but not necessarily essential to any particular website's functioning, and purposes for which a Do Not Track user might not necessarily expect her browsing history to be monitored and retained by third parties with which she has no relationship. Though the working group is agreed that research data could not be used to alter any individual's experience and will ultimately be used in the aggregate, it would be collected and retained on an individualized basis for a potentially extensive period of time (up to 53 weeks per one recent proposal, and longer in others). At one point, the working group had decided to exclude these purposes as a permitted use under the standard, but the idea has recently been reintroduced.[25]

- *Deidentification*: All parties are in agreement that if data has been "deidentified," then it falls outside the scope of Do Not Track. That is, if a set of data has been stripped of identifiers and cannot be attributed to a person or device, Do Not Track should not apply to the data, and the company may use it as it pleases. However, there is debate over how robust deidentification must be. Advocates have argued for a test that largely mirrors the FTC's own test for deidentification: (1) you must have a reasonable belief that data could not be tied back to an individual or device, (2) you must promise not to try to reidentify the data, and (3) anyone you transfer the data to must also promise not to reidentify it. Some working group members have pushed back against this model, arguing that companies should be allowed to retain the technical ability to reidentify data so long as there are institutional controls in place to prevent reidentification. Under that approach, companies could continue to collect behavioral data for research and modeling purposes so long as the company had procedures in place to prohibit anyone within the company from singling out a particular user or device.[26]

- *Browser presentation of Do Not Track options and consequences for non-compliant browsers*: The working group is generally agreed that a Do Not Track signal should represent the will of the user — browsers shouldn't send a Do Not Track signal without the user's understanding and consent. However, there is an open question over who should be able to evaluate the validity of a browser's presentation of Do Not Track choices to users. Some working group participants have argued that third parties should be able to reject Do Not Track signals from browsers that they believe do not adequately obtain consent to turn on Do Not Track from users. Other working group members have argued that third parties

[25] W3C, Tracking Protection Working Group, Tracking Compliance and Scope, Audience Measurement, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#audience-measurement.

[26] W3C, Tracking Protection Working Group, Tracking Compliance and Scope, Unlinkability, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#def-unlinkable.

claiming compliance with Do Not Track should be required to honor syntactically correct signals and not second-guess a user's state of mind.[27]

- *Data retention*: While all parties recognize the need for some level of data collection and retention by third parties when Do Not Track is turned on, there is disagreement on how long companies should be permitted to retain such data. Some working group members have argued that financial and auditing requirements dictate that data should (or must) be retained in individualized form for up to seven years. Other working group members have stated that such extensive retention is neither legally or logistically necessary, and that prolonged and individualized retention of cross-site data would run counter to a user's reasonable expectations in turning on Do Not Track.[28]

Obviously, many of these issues are inter-dependent. Data retention matters more if companies can use unique cookies to log cross-site behavior. Companies may be more willing to adopt a robust deidentification standard if they are allowed to collect and retain data for market research and product improvement. For a bargain to be struck, these issues will all likely need to decided as part of a comprehensive package.

However, to date, most industry working group participants have not been publicly willing to agree to move much beyond the current DAA principles for users who opt out of behavioral advertising, which regulators and advocates have criticized as insufficiently robust.[29] In some ways, industry proposals are even weaker than the rules currently in effect. For example, the DAA code arguably has a stronger definition of deidentification than has been proposed as an alternative within the Tracking Protection Working Group. Indeed, the DAA recently appears to have backtracked on the very notion that Do Not Track should even turn off behavioral advertising — the very purpose for which Do Not Track was originally proposed.[30]

**The Future of Do Not Track and Behavioral Advertising**

Industry's failure to honor Do Not Track signals more than two years after they were first incorporated within Mozilla's Firefox browser is frustrating and perplexing. Despite disagreements over the precise contours of Do Not Track, self-regulatory groups could at least require members to treat Do Not Track as an opt-out under the DAA code, as Yahoo! and some

[27] W3C, Tracking Protection Working Group, Tracking Compliance and Scope, User Agent Compliance, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#user-agent-compliance; W3C, Tracking Compliance Working Group, Tracking Compliance and Scope, Noncompliant User Agents, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#noncompliant-UA.

[28] W3C, Tracking Protection Working Group, Tracking Compliance and Scope, Financial Logging and Auditing, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#financial-logging.

[29] Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, March 2012, http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[30] Email from Rachel Thomas to Tracking Protection Working, October 4, 2012, http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0115.html.

other companies do today.[31] Nor has there been any particular urgency within W3C (or elsewhere) to define a different standard for the treatment of Do Not Track users. Although trade association representatives have increasingly made chicken-little pronouncements on the effect that Do Not Track will have for the web,[32] it is important to remember that they have long supported industry-wide opt-out rights for consumers online. Do Not Track is merely an improvement on industry opt-outs that have not proven sufficiently robust to address user concerns.

Moreover, it is important to note that Safari users have effectively had Do Not Track turned on *by default* for several years, ever since Apple made the decision to prevent third parties from setting cookies. Apple users can readily attest that apocalyptic predictions over the effects of Do Not Track have not come true for them, and that they enjoy the same wide variety of free Web content as users of other browsers, supported by (non-behaviorally targeted) advertisements.

Despite the lack of progress, CDT remains hopeful that ultimately the working group can agree on a strong Do Not Track standard that allows for some basic operational collection and retention of user data but limits behavioral retention and use to whatever is strictly necessary for the web to function. CDT originally proposed such a compromise approach in January 2011 just after the FTC formally called for the adoption of Do Not Track.[33] In April of 2012, we presented a similar compromise suggestion to the Tracking Protection Working Group at a face-to-face meeting in Washington, DC. Under our proposal, third parties would be allowed to use unique identifiers for narrow operational purposes, but not secondary purposes such as market research. We support the robust deidentification standard as articulated by the FTC, but could be willing to allow third parties to reject certain Do Not Track signals — so long as the rejection is immediately signaled to the browser. However, to date, these proposals and other efforts to break the logjam have not gained significant traction.

One important development since Chairman Leibowitz called for Do Not Track in 2010 has been a stronger commitment to user privacy on the part of the browser makers. For years, browser vendors seemed more intent of preserving the business models of behavioral advertising than in satisfying the demands of their users. However, with increased focus on privacy issues by the press and by regulators, browser makers have listened to the demands of their clients — that is, their users — and have increasingly taken steps to protect users' privacy. As noted previously, all the major browser makers have implemented means for users to turn on Do Not Track and send Do Not Track headers to all websites. In June of last year, Microsoft announced that it would include Do Not Track options during the install flow for Windows 8 and Internet Explorer

---

[31] Note however that Yahoo! does not honor Do Not Track requests from Internet Explorer 10, as the company alleges that the user flow for turning on Do Not Track does not sufficiently ensure that the signal represents a user's informed choice. Yahoo! Policy Blog, Shane Wiley, "In Support of a Personalized Experience," October 22, 2012, http://www.ypolicyblog.com/policyblog/2012/10/26/dnt/.

[32] Leslie Harris, "The Bizarre, Belated Assault on Do Not Track," *Huffington Post*, October 4, 2012, http://www.huffingtonpost.com/leslie-harris/the-bizarre-belated-assau_b_1935668.html.

[33] CDT, "CDT Releases Draft Definition of 'Do Not Track,'" January 31, 2011, https://www.cdt.org/blogs/erica-newland/cdt-releases-draft-definition-"do-not-track". CDT subsequently released a slightly revised version of this definition in April 2012, CDT, "What Does 'Do Not Track' Mean? A Scoping Proposal from the Center for Democracy & Technology, April 27, 2011 https://www.cdt.org/files/pdfs/20110447_DNT_v2.pdf.

10 — with the recommended setting set to Do Not Track being on.[34] In February, Mozilla announced that it would join Apple in preventing third parties from setting cookies in its browser.[35]

That browser makers are increasingly competing on privacy and responding to user's sentiments on behavioral advertising[36] is a welcome and important development. For years, privacy advocates have worried that in an arms race between users and ad networks, users, who by and large lack the sophistication and technical skills of the ad networks, were destined to lose. However, with the browsers increasingly acting in accordance with the desires of their user base, that result is no longer a foregone conclusion. Do Not Track was originally offered as a reasonable middle ground to avert an arms race — where ad networks could collect basic operational information and still serve (non-targeted) advertisements.[37] If trade associations continue to stick their heads in the sand and ignore consumer sentiment about their practices (instead of establishing a value proposition to users about behavioral advertising's benefits), moves like Mozilla's and Apple's to frustrate cross-site tracking will become the norm, and an inability to set cookies may be the least of their concerns.

Ultimately, the tortured Do Not Track saga is a stark demonstration of why consumers fundamentally need comprehensive privacy law. Unlike many areas of privacy, behavioral advertising has been under considerable regulatory and press scrutiny for over fifteen years (and intense scrutiny for at least the last five), and still despite all that effort and attention, practices have not meaningfully corrected and aligned with consumer expectations. In order to ensure that adequate consumer protections are in place for behavioral advertising — as well as considerably less examined industries with as least as extensive privacy implications — consumers deserve a strong but flexible horizontal privacy law governing all collection, use, and retention of personal information based on the Fair Information Practice Principles.

Finally, the ever-increasing stores of commercial databases of personal information about each and every one of us provides a compelling reason to revisit law enforcement privacy rules as well. For this reason, CDT has convened the Digital Due Process coalition to advocate for the reform of the Electronic Communications Privacy Act, to ensure that these databases are only accessed by the government under the due process of law.[38] Absent meaningful protections on potential government abuse, consumers have all the more reason to distrust commercial data collection and retention practices.

---

[34] Ed Bott, "Microsoft sticks to default Do Not Track settings in IE 10," *ZDNet*, August 7, 2012, http://www.zdnet.com/microsoft-sticks-to-default-do-not-track-settings-in-ie-10-7000002289/.

[35] Justin Brookman, CDT blog, "Mozilla Says Enough is Enough," February 26, 2013, https://www.cdt.org/blogs/justin-brookman/2602mozilla-says-enough-enough.

[36] Joseph Turow *et al.*, "Americans Reject Tailored Advertising and Three Activities that Enable It," September 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214; Wendy Davis, "Zogby Poll: Web Users Troubled by Behavioral Advertising," *MediaPost*, June 8, 2010, http://www.mediapost.com/publications/article/129753/#axzz2REncGaSy.

[37] Leslie Harris, "The Bizarre, Belated Assault on Do Not Track," *Huffington Post*, October 4, 2012, http://www.huffingtonpost.com/leslie-harris/the-bizarre-belated-assau_b_1935668.html.

[38] Digital Due Process, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

## Conclusion

CDT would like to thank Senator Rockefeller and the Committee again for holding this important hearing on an issue that Americans are increasingly concerned about. We believe that Congress has a critical role to play in ensuring the privacy of consumers, through rigorous oversight of industry practices, and through the long overdue enactment of reasonable privacy legislation. CDT looks forward to working with the Members of the Committee as they pursue this and other privacy issues further.