W3C Workshop on Do Not Track and Beyond-Position Paper
Chris Jay Hoofnagle & Jennifer M. Urban

We recently commissioned a national survey focusing upon information privacy that examined several online privacy issues. Among them was the Do Not Track proposal. Our full paper is available online,[1] and we excerpt the main findings here.

Use versus collection

In our pretest of survey questions, we asked respondents what DNT meant, but almost two-thirds of the respondents simply did not know. Indeed, the vast majority of American consumers have never heard of DNT.

As a result of the pretest, we changed approaches, and instead of asking what they expected DNT would do, we asked consumers what they preferred it do. We also explicitly asked the full sample whether DNT was something they had heard of, or not.

We asked American consumers, "Policymakers are considering creating a “do not track” option for the internet. Have you heard of proposals for a “do not track” system, or not?" Thirteen percent had heard of it, and fully 87 percent had not. (N=1203.)

We then asked what Americans would prefer Do Not Track to do. Three options were presented to respondents in random order. One option would prevent collection of information; the other two would prevent two different actions on the part of the website.

A majority—60 percent—said they wanted DNT to stop websites from collecting information about the user. This was the closest option to the FTC’s proposal and the proposals of privacy groups, although simplified. The next largest group, 20 percent, wanted DNT to block advertisements. We presented that option because we suspected that many users expected DNT to simply block ads. Only 14 percent chose

[1] Chris Jay Hoofnagle, Jennifer Urban and Su Li, *Privacy and Modern Advertising: Most US Internet Users Want “Do Not Track” to Stop Collection of Data About their Online Activities*, Amsterdam Privacy Conference 2012, Oct. 8, 2012, available at http://ssrn.com/abstract=2152135.

the option that most closely matches the industry's suggested use-restriction proposal.

Tracking on medical websites

Medical information is recognized as particularly sensitive. It is one of the few data types explicitly protected under federal law. As early as 2000, the advertising industry itself recognized the sensitive nature of medical information and promised not to use it for advertising. In July 2000, the major network advertising companies[2] articulated the Network Advertising Initiative (NAI) "Self-Regulatory Principles for Online Preference Marketing by Network Advertisers." Under this framework, the NAI promised to not use "sensitive" personally identifiable data for "online preference marketing." The group explained, "Network advertisers shall neither use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, nor social security numbers, for OPM [online preference marketing]."[3]

Almost ten years later, the advertising industry has retreated from its 2000 position, and the 2000 principles can no longer be found on the NAI's website.

When we turned to tracking on medical websites in this survey, we found that large numbers of consumers do not know what the rules are. We asked respondents whether it was true or false that advertisers are not allowed to track users using the internet to learn about medical conditions. While 36 percent correctly answered that this statement was false, 63 percent either did not know or responded incorrectly. Specifically, 22 percent thought permission was necessary, and 41 percent said they did not know the answer.

Attitudes toward online advertising

We first asked, "In general, how often do you find online advertising, such as the advertising that appears on search results webpages and banner advertisements, useful?" Thirty percent do find utility in

[2] 24/7 Media, AdForce, AdKnowledge, Avenue A, Burst! Media, DoubleClick, Engage, L90, MatchLogic.
[3] http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf.

advertising, with 10 percent reporting that they find search and banner advertisements useful often, and 20 percent sometimes find this information useful. Thirty-six percent answered "hardly ever," and 33 percent answered "never."

We followed the utility question by asking whether users actually clicked on advertisements. We asked, "How often do you click on advertisements when using the internet?" Fifty percent claimed that they never click on ads, and 35 percent responded hardly ever. It may be that this is incorrect—that consumers do not remember or selectively remember their interaction with advertising.[4] We have no way to test this directly; however, there is some indirect evidence supporting our respondents' claims. It is true, for example, that accidental and fraudulent clicks are a pervasive problem,[5] and that as of this writing, the most popular add-on for the Firefox web browser is AdBlock Plus, with over 14 million users.

Conclusion

In light of consumer attitudes and marketplace realities, Do Not Track is a modest intervention. Yet the advertising industry has argued for systemically weakening what "Do Not Track" means, and has retreated from earlier, stronger promises to limit tracking.

We found that most consumers want Do Not Track to mean exactly that: do not collect information that allows companies to track them across the Internet. This may seem obvious, but even the definition articulated by the FTC may fall short of these consumer expectations. Further, advertising industry groups presently are lobbying for a different interpretation that would allow pervasive tracking and use of information derived from online experiences, even if the consumer opts out.

---

[4] We note that we did not have a way to verify whether this claim is borne out by actual behavior, but it is clear that our respondents subjectively found online ads of limited value.

[5] Ryan Kim, Report: *40 Percent of Mobile Clicks are Fraud or Accidents*, GIGAOM, Aug. 31, 2012, *available at* http://gigaom.com/2012/08/31/report-40-percent-of-mobile-clicks-are-fraud-or-accidents/

This disconnect appears pervasive and strong. In addition to the fact that a strong majority of respondents prefer that Do Not Track allow them to opt out of collection, there is a lack of understanding about what trackers can do. We found that only about 1 in 5 internet users understands that advertisers can track them on medical sites. Here too, despite broad consensus that medical information is especially sensitive and despite widespread consumer ignorance of the rules governing the collection and use of behavioral tracking on medical websites, advertising lobbying groups have stuck to a "notice and no choice" approach.

Consumers and advertisers seem to be at an impasse on privacy. This impasse is the product of consumers' anxiety about tracking, and advertisers' concern that any imposition upon data collection will undermine an existing and growing business model. Subjectively at least, nearly 70% of consumers say that they find little if any value in online ads. Half claim to never click on ads at all. Yet advertisers' position on tracking is that consumers should be tracked even if they opt out of tracking, suggesting that consumers' subjective opinions about tracking do not matter.

Lost in the present debate is the fact that DNT essentially responds to a specific business model, one in which third parties attempt to build advertising value by tracking individuals in all aspects of their lives. This model seems to require continually ratcheting up data collection and ratcheting down privacy protections in an attempt to show value to ad buyers.

Targeting consumers based upon specific information about them appears to be increasing across a variety of internet and mobile marketing models, with an apparent goal of linking online and offline purchase behavior. In previous work, we have explored mobile payments models that promise to connect more payments ecosystem players with detailed "Level 3" purchase data (lists of the specific things consumers buy) for individual consumers shopping at bricks-and-mortar stores and mobile app models that use app users' address books to target offers.[6] And as this paper was being prepared, for

[6] Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, *Mobile Payments: Consumer Benefits & New Privacy Concerns* (Apr. 24, 2012); and Jennifer M.

example, newspapers reported that Facebook was beginning to buy data on Facebook users' specific purchases in CVS drugstores in order to show whether targeted ads served to individual profiles actually resulted in increased sales of the advertised products.[7]

If present trends continue, we will soon find ourselves in a world where ultra-large tracking platforms will have data about almost all online and offline consumer transactional behavior. Consumers will find themselves subject to these platforms' power to collect and use that data, and with little recourse or say about that collection and use.

We think that there are ways around the impasse between advertising models and consumers' apparent expectations of privacy. There are alternative approaches to the "track everyone, everywhere" model. Academics including Steven Bellovin,[8] Eric Goldman,[9] and Helen Nissenbaum[10] have proposed alternative models that would allow highly targeted ads without creating dossiers of internet behavior held by third parties.

Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privacy* (July 12, 2012), *available at* http://ssrn.com/abstract=2103405.

[7] Rebecca Greenfield, *Facebook Now Knows What You're Buying at Drugstores*, THE ATLANTIC WIRE (Sept. 24, 2012), *available at* http://www.theatlanticwire.com/technology/2012/09/facebook-tracking-you-drug-store-now-too/57183/.

[8] Elli Androulaki and Steven M. Bellovin, *A secure and privacy-preserving targeted ad-system*, *in* Proceedings of the 1st Workshop on Real-Life Cryptographic Protocols and Standardization, Jan. 2010.

[9] Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151 (2006).

[10] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, Solon Barocas, *Adnostic: Privacy Preserving Targeted Advertising*, NDSS 2010, *available at* http://crypto.stanford.edu/adnostic/.