ITIF
The Information Technology & Innovation Foundation

Policymakers Should Opt Out of "Do Not Track"

BY DANIEL CASTRO | NOVEMBER 2010

"Do Not Track" would impose unnecessary costs on software developers, result in more intrusive and less relevant advertising for consumers, and, if widely adopted, significantly harm the current funding mechanism for the Internet ecosystem.

For the last few years privacy fundamentalists have called for a national Do Not Track feature for online advertising modeled after the national Do Not Call Registry. The purpose of a Do Not Track feature would be to provide consumers a single, centralized mechanism to opt out of all online profiling for targeted advertising. However, such a mandate would impose unnecessary costs on software developers, result in more intrusive and less relevant advertising for consumers, and, if widely adopted, significantly harm the current funding mechanism for the Internet ecosystem, resulting in less free Internet content and services.

While the Do Not Track proposal is not new, it has received renewed attention in recent months. FTC chairman Jon Leibowitz testified in July 2010 that the Commission was exploring this proposal in its upcoming report on privacy and FTC Commissioner Julie Brill endorsed the Do Not Track proposal in October 2010.[1] A coalition of privacy organizations, including the Center for Democracy and Technology (CDT), the Electronic Frontiers Foundation (EFF), and the World Privacy Forum, first began advocating for the Do Not Track proposal in 2007. These groups reasoned that since consumers benefited from the popular Do Not Call regulations for telemarketing, consumers would similarly benefit from Do Not Track regulations for online advertising. While the proposal may be intriguing at first glance, a closer look reveals that the idea is illogical, impractical, and would hurt, not help, consumers.

HOW DO NOT TRACK WOULD WORK

Understanding the problems with Do Not Track first requires understanding how such a proposal could work. Comparisons between Do Not Call and Do Not Track are not useful from a technical perspective. The Internet is not the same as the telephone network. Individuals do not have a single unique identifier on the Internet. The closest unique identifier to a telephone number on the Internet is an Internet Protocol (IP) address, but users share and change IP addresses frequently which would render any IP-based opt-out list impractical.

A mandate by Congress to implement a Do Not Track mechanism would therefore have to be fulfilled through other means, including through changes in Internet browsers and other Internet-connected applications that show ads or modifications to the HTTP standard. CDT, which endorsed the Do Not Track idea in 2007, suggested the former.[2] They proposed that advertisers be required to provide the FTC a list of the domain names used to set persistent unique identifiers and track users across multiple websites. In addition, companies that make Web applications such as web browsers and plug-ins would have to develop new functionality to block these domains and keep the list up-to-date.

An alternative implementation for Do Not Track would require modifying the HTTP protocol used for web browsing so that users could signal to the web server that they do not want to be tracked. The server would in turn be required to detect this flag and then refrain from setting any unique persistent identifiers for that particular user. Implementing this for all users would require that all software using HTTP be updated to the new standards. This proposal would only apply to HTTP traffic. Non-HTTP applications that use targeted ads would require a separate implementation. Clearly, such a change would require substantial retooling of existing websites, web browsers and other related software, the costs of which would ultimately be borne by consumers, the majority of which are not bothered by targeted advertising on the Internet.[3]

WHY DO NOT TRACK IS A BAD IDEA

Although comparisons are often made between the two, there are many differences between the existing National Do Not Call Registry and the Do Not Track proposal. The National Do Not Call Registry, managed by the Federal Trade Commission (FTC), is designed to reduce the amount of unwanted telemarketing phone calls that consumers receive. The purpose is to make it easier and more efficient for consumers to stop getting unwanted telemarketing calls.[4]

In contrast (and somewhat ironically) the Do Not Track proposal would have the opposite effect of the National Do Not Call Registry since users who opt out of tracking would receive more, not less, unwanted advertising. Do Not Track would not stop online advertising, but rather would limit advertisements based on an individual's interests thus increasing the amount of irrelevant (and therefore unwanted) advertising for each user that opts out. In addition, advertisers would likely resort to overlay and pop-up ads which users may find annoying but are more effective at getting their attention. As Goldfarb and Tucker found in a study of the impact of European privacy regulations on online advertising, small, text-based ads are significantly less effective unless they can be tailored to

a user's interests.[5] Targeted advertisements are more effective (since they are relevant to the individual) and generate more revenue for online services.[6] Unlike niche websites that focus on a particular topic or demographic, without learning more information about users, general interest websites like online newspapers cannot deliver targeted ads to users since they know very little about the interests of each individual.

Another problem with Do Not Track is that it does not scale well on the global Internet. As described above, to be effective, the proposal would require a federal mandate calling for substantive modifications to networking protocols, web browsers, software applications and other Internet devices. Besides raising costs for consumers, it is unclear how effective such a mandate would be outside of the U.S. borders or how well the proposal would be received by international standard bodies.

If a Do Not Track list ever became widely implemented companies could respond by simply blocking access to those sites for users who opt out, just as some sites today block users who use ad-blocking software or do not register on a site.[7] Users who currently opt out of targeted advertising but continue to use the content or service which the advertising pays for are essentially free riders. They are the minority of users who are benefitting from the willingness of the majority to divulge some personal information in exchange for free or reduced-price content. It is this exchange that enables the U.S. Internet ecosystem to be so robust and largely free of charge to the average user. Privacy advocates rarely acknowledge the harm to advertising revenues that would result from a large number of consumers signing up for Do Not Track.

This is why the analogy to Do Not Call is fundamentally flawed. When consumers choose to opt out of unsolicited telemarketing calls they are not at the same time receiving some free service that is linked to the telephone call. It would be one thing if, for example, the daily newspaper company said in exchange for a free newspaper every day we get to call your house every evening at dinner time. But that is not the deal. There is no quid pro quo. These unsolicited calls are simply an added cost to the economy and an annoyance to most consumers.

In contrast, Do Not Track is like getting the free newspaper without taking the calls. When consumers go online, in the vast majority of cases they are receiving some free content or service (e.g., email, search, data storage, social networking, news, information, entertainment, etc.). And the way they "pay" for these free services is by agreeing to be shown advertisements. And to cover the cost of all of these services companies increasingly need to show ads that are actually of interest to consumers. By opting out of this mutually beneficial relationship, consumers are trying to get something for nothing.

This is not to say that consumers should not be able to avoid targeted advertising. The way to do that is to not access sites that display this type of advertising. However, just as users cannot "opt out" of paying for a magazine at a newsstand, users should not be able to opt out of targeted advertising and still receive access to the free content. Similarly, customers at a grocery store who use a loyalty card receive a discount and those who choose to keep their shopping behavior private do not. Of course privacy fundamentalists pushing for Do Not Track want to have their cake and eat it too. If the marketplace ever evolved to the

point where website operators only made content available to individuals who permit targeted advertising, many privacy advocates would likely start clamoring for legislation to prevent companies from "discriminating" against users who opt out of targeted advertising.[8]

Finally, policymakers should remember that online privacy is complex. While some users may not want certain online activities (e.g. online medical research) tracked and used to deliver targeted ads, others may welcome this advertising (e.g. ads targeted to their health concerns). Similarly, some users may consent to receiving targeted ads based on their activity on a single website but not based on their activity across different websites. Depending on how Do Not Track is applied it could limit targeted advertising to information gathered on a single domain but prohibit targeted advertising across multiple domains. This may allow sites like Amazon.com or Facebook which have large databases of user information to continue to provide targeted advertising but would likely hurt the ability of smaller publishers who rely on third-party advertising networks to deliver personalized ads. A government-imposed, one-size-fits-all solution for privacy will not provide users what they want.

CONCLUSION

Do Not Track is just another attempt by privacy fundamentalists to kill behavioral advertising which they find repugnant and invasive. Indeed, some of the "consumer advocates" behind Do Not Track seem to oppose advertising in general as predatory and anti-consumer.[9] If the goal of the initiative is to restrict targeted advertising, it would be better for Congress to just ban Internet advertising outright and develop a "Corporation for Public Internet" to fund Internet content and applications.

Do Not Track does not actually solve the primary privacy concern that most people have: that their personal information will be used to unfairly harm or disadvantage them. If the goal is to protect consumers from harm, instead of a Do Not Track list, the government would be better off creating a Do Not Harm list. With a Do Not Harm list, organizations would not be permitted to take discriminatory or other harmful actions against individuals who register on this list. Imagine the possibilities: Do you not want your employer to fire you based on health information discovered about you online? Do you not want your bank to raise your credit card interest rates based on financial activity it managed to glean from your web browsing history? Do you not want the government to spy on your personal shopping history? Then sign up for the Do Not Harm list!

Of course it is clear that such a list is unnecessary—all citizens should be protected from basic discriminatory and harmful activities by businesses and government. But it is impossible to eliminate all risk of a security breach and so some private consumer data will unfortunately always end up being exposed as a result of security failures. The goal should be to minimize the impact and frequency of these incidents. And that should be the purpose of government privacy regulations—to promote good security practices, to create and clarify the protections available to citizens, to define recourses available to them in case of a privacy breach, and to institute policies that will minimize harms when sensitive data is known about them.

The Internet ecosystem is a significant source of economic activity in the United States (accounting for approximately $300 billion in activity, or roughly 2 percent of GDP[10]) and online advertising is the fuel powering this economic dynamo.[11] Policymakers should consider carefully any attempts to limit the use of online advertising and its effect on the Internet at large before tampering with the foundation of its growth.

ENDNOTES

1. Jon D. Leibowitz, "Consumer Online Privacy," Testimony before the U.S. Senate Committee on Commerce, Science and Transportation, July 27, 2010 and Julie Brill, "Remarks by Commissioner Julie Brill United States Federal Trade Commission," Proskauer on Privacy, October 19, 2010, http://www.ftc.gov/speeches/brill/101019proskauerspeech.pdf.
2. "Operation of the Do Not Track List," Center for Democracy and Technology, October 31, 2007, http://www.cdt.org/privacy/20071031donottrack.pdf.
3. One such implementation of an HTTP header is described here: Harlan Yu, "Do Not Track: Not as Simple as it Sounds," Freedom to Tinker, August 10, 2010, http://www.freedom-to-tinker.com/blog/harlanyu/do-not-track-not-simple-it-sounds.
4. The National Do Not Call Registry does not limit all telemarketing—calls from political organizations, charities and telephone surveyors are permitted as well as calls from organizations from which the consumer has purchased an item in the previous 18 months.
5. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
6. Howard Beales, "The Value of Behavioral Targeting," 2009, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
7. Sites like the Washington Post and the New York Times require users to register to access content. ArsTechnica ran an experiment where it blocked users who were running ad blocking software for 12 hours. Ken Fisher, "Why Ad Blocking is devastating to the sites you love," ArsTechnica, March 2010, http://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars.
8. A sample post along these lines can be found here: http://activerhetoric.wordpress.com/2010/11/08/do-not-track-means-do-not-track/
9. "Online Behavioral Tracking and Targeting: Legislative Primer September 2009," Center for Digital Democracy, September 2, 2009, http://www.democraticmedia.org/doc/privacy-legislative-primer.
10. John Deighton and John Quelch, "Economic Value of the Advertising-Supported Internet Ecosystem," Hamilton Consultants, June 10, 2009, http://www.iab.net/media/file/Economic-Value-Report.pdf.
11. Daniel Castro, "Stricter Privacy Regulations for Online Advertising Will Harm the Free Internet," Information Technology and Innovation Foundation, September 2010, http://www.itif.org/files/2010-privacy-regs.pdf.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with ITIF specializing in information technology (IT) policy. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security and accessibility. He has experience in the private, non-profit and government sectors. Mr. Castro has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity

FOR MORE INFORMATION CONTACT ITIF BY PHONE AT 202.449.1351, BY EMAIL AT MAIL@ITIF.ORG, OR VISIT US ONLINE AT WWW.ITIF.ORG.