Statement for the Record of
The Electronic Privacy Information Center (EPIC)

Marc Rotenberg, EPIC President
Sharon Goott Nissim, EPIC Consumer Protection Fellow

Hearing on
"Do Not Track Legislation: Is Now the Right Time?"

Before the
Committee on Energy and Commerce;
Subcommittee on Commerce, Trade and Consumer Protection;
U.S. House of Representatives

December 2, 2010
2123 Rayburn House Office Building
Washington, D.C.

Mr. Chairman, Members of the Committee, this statement was prepared for the hearing "Do Not Track Legislation: Is Now the Right Time?" held on December 2, 2010 before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection. We ask that it be included in the hearing record.

The Electronic Privacy Information Center (EPIC) is a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has long focused on the impact of emerging technologies on privacy. And I was directly involved in the development of the Telephone Consumer Protection Act of 1991 and the Do Not Call program that followed, which established a meaningful and effective way for consumers to opt-out of telemarketing calls.

EPIC supports the Committee's examination of Do Not Track proposals. It is important to recognize that as the Internet has expanded, so have the invasions of consumer privacy, in the form of data collection and behavioral targeted advertising. EPIC recommends that the Committee evaluate the Do Not Track proposal in light of the lessons from past efforts to safeguard consumers from unwanted advertising and marketing.

I. The History of the Telephone Consumer Protection Act (TCPA) and Do Not Call List

In this current debate over a Do Not Track system for the Internet, it is helpful to look back and examine previous debates over the Telephone Consumer Protection Act and the Do Not Call List. While any future Do Not Track mechanism may look different from the Do Not Call registry, many of the issues encountered then are still relevant now.

A. The Telephone Consumer Protection Act (TCPA)

The Telephone Consumer Protection Act, 42 U.S.C. § 227, was passed in 1991. This Act amended the Communications Act of 1934 to prohibit automated and prerecorded telephone calls to the home, as well as the sending of unsolicited fax messages.[1] The Act directed the Federal Communications Commission (FCC) to initiate a rulemaking proceeding concerning the need to protect peoples' privacy rights to avoid receiving telephone solicitations they do not want, including the possibility of establishing a single national database compiling a list of those residents who object to such phone calls.[2] The Act allowed states to bring civil suits to enforce the law,[3] but gave exclusive jurisdiction over these actions to federal district courts,[4] and also provided for a private right of action.[5]

[1] 42 U.S.C. § 227.
[2] 42 U.S.C. § 227 (c)(1)(A).
[3] 42 U.S.C. § 227 (f)(1).
[4] 42 U.S.C. § 227 (f)(2).
[5] 42 U.S.C. § 227 (c)(5).

B. The Creation of the Do Not Call Registry

The FCC, as directed by the TCPA, initiated a rulemaking on the idea of a Do Not Call registry and other related matters.[6] EPIC, along with ten other advocacy groups, submitted comments urging the creation of a telemarketing "do not call" registry.[7] The comments identified the public's frustration with the "intrusion into the privacy of the home," of unwanted telephone solicitations, and described how difficult it was under the current rules for individuals to prevent these type of calls, especially in light of changing technologies.[8] Additionally, the comments laid out the legal reasoning as to why the FCC's proposed regulations were consistent with First Amendment principles.[9]

The EPIC comments also pointed out, however, that an opt-in system requiring express consent from individuals before telemarketers could initiate sales calls would be preferable to the opt-out regime that a Do Not Call registry imposes. "An opt-in framework," the comments explained, "would better protect individuals' rights and is consistent with most United States privacy law."[10] The EPIC comments argued further that opt-in is more effective "because it encourages companies to explain the benefits of information sharing, and to eliminate barriers to exercising choice . . . [e]xperience with opt-out has shown that companies tend to obfuscate the process of exercising choice, or that exemptions are created to make opt-out impossible."[11]

The FTC also proposed the Telemarketing Sales Rule (TSR),[12] which included a do not call list, and received similar favorable comments from EPIC and other groups in response.[13] These new FTC regulations required telemarketers to transmit caller ID information, establish new rules for the use of preacquired account number information, and prohibit "abandoned" calls.[14]

---

[6] FCC Notice of Proposed Rulemaking on the TCPA, Oct. 8, 2002, *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-25569-filed.

[7] Comments of EPIC, et al. before the FCC, in the matter of "Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991," Dec. 9, 2002, *available at* http://epic.org/privacy/telemarketing/tcpacomments.html.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] Federal Trade Commission, Telemarketing Sales Rule, 16 CFR Part 310, *available at* http://www.ftc.gov/os/2002/12/tsrfinalrule.pdf.

[13] Comments of EPIC et al, before the Federal Trade Commission, in the matter of Telemarketing Rulemaking – Comment, April 10, 2002, *available at* http://epic.org/privacy/telemarketing/tsrcomments.html.

[14] Federal Trade Commission, Telemarketing Sales Rule, 16 CFR Part 310, *available at* http://www.ftc.gov/os/2002/12/tsrfinalrule.pdf.

In March 2003, Congress passed legislation allowing the FTC to operate a national Do Not Call List.[15] This legislation approved the levying of fees on the telemarketing industry in order to fund this program.[16] In June of 2003, the National Do Not Call Registry opened for enrollment and registration exceeded 10 million on the first day.[17] Registry enforcement is coordinated between the FCC and the FTC according to a memorandum of understanding.[18] As of October 2003, 53.7 million numbers were registered on the Do Not Call list and consumers had filed 15,000 complaints against telemarketers who did attempt to call them.[19]

Originally the FTC adopted a five-year re-registration mechanism for the Do Not Call list to ensure it was accurate.[20] However, the FTC has successfully used a scrubbing program to purge the Registry of disconnected and reassigned numbers each month.[21] This program, along with the increased use of cell phones and the popularity of telephone number portability, made the re-registration procedure less necessary than it had been when it was adopted.[22] On October 23, 2007, the FTC testified before Congress that "it will not drop any telephone numbers from the Do Not Call Registry based on the five-year expiration period pending final Congressional or agency action on whether to make registration permanent."[23]

C. Legal Challenges to Do Not Call

Industry groups immediately responded to the creation of the Do Not Call registry by filing lawsuits. Several lawsuits were filed, arguing that the Do Not Call registry was unconstitutional under the First Amendment because it did not protect corporate telemarketers' "commercial speech" and the exclusion of non-commercial charitable

---

[15] "Do Not Call Implementation Act," Public Law 108-10.
[16] *Id.*
[17] Federal Trade Commission, June 17, 2003, "Do Not Call Registrations Exceed 10 Million," *available at* http://www.ftc.gov/opa/2003/06/dncregistration.shtm.
[18] *See* FTC Annual Report to Congress, FY 2003 and 2004, "Pursuant to the Do Not Call Implementation Act on Implementation of the National Do Not Call Registry," Appendix – FTC-FCC Memorandum of Understanding on Telemarketing Enforcement.
[19] FTC, "Consumers on Do Not Call Registry File Over 15,000 Complaints Against Telemarketers," Press Release, October 16, 2003, *available at* http://www.ftc.gov/opa/2003/10/dnccomplaints.shtm.
[20] *See generally,* EPIC: Do Not Call, *available at* http://epic.org/privacy/telemarketing/dnc/.
[21] *Id.*
[22] *Id.*
[23] Statement of the Federal Trade Commission, "Enhancing FTC Consumer Protection in Financial Dealings, with Telemarketers, and on the Internet," before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, U.S. House of Representatives, Washington. D.C, Oct. 23, 2007, *available at* http://www.ftc.gov/os/testimony/071023ReDoNotCallRuleEnforcementHouseP034412.pdf.

organizations from the registry amounted to a "content-based" speech restriction.[24] The suits also charged that the FTC did not have authority to enact these rules.[25]

In February 2004 in a consolidated appeal of these suits, the U.S. Court of Appeals for the Tenth Circuit upheld the FTC's Do Not Call Registry.[26] The Court held that the Do Not Call registry did not violate the First Amendment, the registry is a reasonable restriction on commercial speech,[27] and "commercial calls were more intrusive and posed a greater danger of customer abuse."[28] The Court also found that the FTC had the authority to create and operate the list, and could levy fees on telemarketers for its operation.[29]

II. Online Advertising and Privacy

This section presents an overview of the current problems in online tracking and targeted advertising. Marketing has come a long way from telephones, and online advertisers use a variety of web-based tactics to track consumers' online behavior and target ads based on that behavior.

A. Data Collection

There is a giant chasm between the type of tracking that companies are engaged in on the web and what people know or think is occurring. The general public has very little idea that every second they are on the Internet, their behavior is being tracked and used to create a "profile" which is then sold to companies on "stock-market-like" exchanges.[30] According to a Wall Street Journal study, the nation's top five websites installed an average of 64 pieces of tracking technology onto the computers of visitors, usually without warning, for a total of 3,180 tracking files. A dozen sites installed more than a hundred.[31] Two-thirds of those files installed by 131 companies that are in the tracking and online consumer profiling business.[32]

Online tracking is no longer limited to the installation of the traditional "cookies" that record websites a user visits. Now, new tools can track in real time the data people are accessing or browsing on a web page and combine that with data about that user's

---

[24] *See* Mainstream Marketing Services, Inc. v. FTC, 283 F.Supp.2d 1151 (D. Colo. 2003); U.S. Security v. FTC, 282 F.Supp.2d 1285 (W.D. Okla. 2003).
[25] *Id.*
[26] Mainstream Marketing Services, Inc., et al. v. Federal Trade Commission, et al., 358 F.3d 1228 (10th Cir. 2004), *available at* http://www.epic.org/privacy/telemarketing/03-1429.pdf.
[27] *Id.* at 1237-39 (finding substantial government interest in "1) protecting the privacy of individuals in their homes, and 2) protecting consumers against the risk of fraudulent and abusive solicitation," and a reasonable fit between the rules and these interests).
[28] *Id.* at 1233.
[29] *Id.* at 1246-50.
[30] Julia Angwin, "The Web's New Gold Mine: Your Secrets," What They Know Series, THE WALL STREET JOURNAL, July 30, 2010.
[31] *Id.*
[32] *Id.*

location, income, hobbies, and even medical problems.[33] These new tools include flash cookies and beacons. Flash cookies can be used to re-install cookies that a user has deleted, and beacons can track everything a user does on a web page including what the user types and where the mouse is being moved.[34]

Advertisers are no longer limited to buying an ad on a targeted website because they are now paying to "follow people around the Internet, wherever they go, with highly specific marketing messages."[35] Companies then use this information to decide what credit-card offers or product pricing to show people, potentially leading to price discrimination.[36]

B. Privacy Issues

This type of data collection violates several Fair Information Practices (FIPs).[37] These online tracking companies have no transparency – so there is no way for a user to access the data being collected about him or her, or correct any inaccuracies. And even if users were to somehow be able to find out what information was being collected, they have no control over what the data collecting companies subsequently do with that information.

According to the Consumer Federation of America and Consumers Union, "there is a fundamental mismatch between the technologies of tracking and targeting and consumers' ability to exercise informed judgment and control over their personal data."[38] The information being collected online is not information that consumers voluntarily share with these tracking companies or online advertising businesses. There are no regulations or limits on what can be collected.

Very sensitive information is often collected, including health and financial data. One company, Healthline, lets advertisers track people with bipolar disorder, overactive bladder, or anxiety – producing ads related to those conditions targeted at specific people.[39] Advertisers collect, use, and sell social security numbers, financial account numbers, and information about sexual behavior and sexual orientation with no controls or limits.[40]

---

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Emily Steel and Julia Angwin, "On the Web's Cutting Edge, Anonymity in Name Only," What They Know Series, THE WALL STREET JOURNAL, August 4, 2010.
[37] Code of Fair Information Practices, *available at* http://epic.org/privacy/consumer/code_fair_info.html.
[38] CFA and CU comments to the FTC concerning the Proposed Online Behavioral Advertising Self-Regulatory Principles, April 11, 2008, *available at* www.ftc.gov/os/comments/behavioraladprinciples/080411cfacu.pdf.
[39] Angwin, *supra* note 30.
[40] CFA and CU comments, *supra* note 38 at 4.

Another consequence of online data collection is the possibility that all these "anonymized" pieces of data could actually be used to identify a person. In the Wall Street Journal, a researcher described how all that is needed to "de-anonymize" data is 33 "bits" of information (some more valuable than others) – and one exemplar website transmitted 26.5 bits of information about a user – enough to narrow the user down to one of just 64 people in the world.[41]

C. Lack of Action

So far, online advertising and behavioral tracking companies have been allowed to operate unchecked. The FTC has relied on "notice and choice" and self-regulation as their tools of choice. But neither of these is effective at protecting consumers' privacy. Privacy policies and notices do not work; less than one percent of consumers read these statements, and even those who do read them do not generally assume that their information is shared with others or combined with information from other sources to form a profile.[42]

And self-regulation certainly is not the answer. The companies engaged in these tactics will not voluntarily decide to curtail them – not when it means less revenue. When given the chance, companies tend to obfuscate the process of exercising choice, or ensure that exemptions are created to make meaningful choice or opt-out impossible.[43] A group called the Network Advertising Initiative (NAI), composed of 11 advertiser members, says the industry polices itself and people can download an opt-out cookie.[44] However, not all behavioral advertising companies join this initiative, and, more importantly, the opt-out process is technically difficult and requires a different download for each advertising company from which a user wishes to opt-out.[45] In fact, as EPIC has earlier noted, the NAI "opt-out cookie" is counterintuitive because it requires consumers who are seeking to protect their privacy to download and retain a tracking technique when the better practice would be to simply delete all advertising related cookies.

"If you look back at the Do Not Call list it was at one time managed by industry," stated Pam Dixon, director of the World Privacy Forum.[46] "The industry has had seven years to prove they can manage online opt-outs. It is time to move toward something structured like the Do Not Call List to address the problems we are seeing and have now

---

[41] Steel and Angwin, *supra* note 36. ("bits" include income level, education, geographic location, zip code, birthdate, etc.)
[42] *Id.*
[43] Comments of EPIC, et al. before the FCC, *supra* note 7 at 4.
[44] *See* "Opt-Out of Behavioral Advertising," Network Advertising Initiative, *available at* http://www.networkadvertising.org/managing/opt_out.asp.
[45] Catherine Rampell, "'Do Not Track' Registry Proposed for Web Use: Online Behavior Used to Tailor Ads," THE WASHINGTON POST, November 1, 2007.
[46] Ryan Singel, "Privacy Groups Asks for Online 'Do Not Track' List," Wired, Oct. 31, 2007, *available at* http://www.wired.com/politics/onlinerights/news/2007/10/do_not_track

seen for seven years."[47] In other words, self-regulation has not worked in other consumer protection areas, and there is no reason to believe that it would work here.

EPIC believes that key to an effective Do Not Track initiative must include the adoption of legislation that makes a consumer's decision to opt out of tracking enforceable, persistent, transparent, and simple.

III. Do-Not-Track Proposals

There are several strategies for implementing a Do Not Track system. Earlier proposals focused on registries akin to the Do Not Call list. The most recent proposals head in a different, and possibly more effective, direction.

A. User-Registry Approach

This approach would allow individual users to register for a do-not-track list with some unique identifier, presumably their IP address. This approach has several significant drawbacks. First, there really are no "universally recognized user identifiers" being used on the web.[48] "By mandating a global, robust identifier," the *33 bits* blog explains, "a user registry would in one sense *exacerbate* the very problem it attempts to solve."[49] This approach would also not allow a user to change do not track settings from site to site.[50]

Second, if IP addresses were used as the identifier, new problems emerge. IP addresses are often dynamic, and several devices can share the same IP address.[51] Moving to static IP addresses to enforce a Do-Not-Track system would ironically make it easier to track the activities of Internet users since the fixed IP would now operate as an "Internet SSN," and become a de facto identifier for a lot of user activity. If the registry is somehow cookie-based, then it would apply only to the browser and not the individual using it and users would have to register all their computers.[52]

---

[47] *Id.*
[48] "'Do Not Track' Explained," September 20, 2010, 33 Bits of Entropy, *available at* http://33bits.org/2010/09/20/do-not-track-explained/.
[49] *Id.*
[50] *Id.*
[51] Harlan Yu, "Do Not Track: Not as Simple as It Sounds," CircleID: Internet Infrastructure, Aug. 10, 2010, *available at* http://www.circleid.com/posts/do_not_track_not_as_simple_as_it_sounds/.
[52] Marc Roth, "The Do Not Track List and the Law of Unintended Consequences," E-COMMERCE TIMES, Oct. 16, 2010, *available at* http://www.ecommercetimes.com/story/71048.html?wlc=1291046770.

B. Domain-Registry Approach

This approach requires advertisers that track online behavior to report what servers or domains they use to do their tracking to some authority such as the FTC.[53] Users would then have to download a plug-in for their browsers that would block the domains on the centralized list.[54] The problems with this approach are: 1) the centralization would be difficult to accomplish; 2) blocking tracking domains might block all advertisements (because showing an ad on a website necessitates contacting the hosting server); and 3) consumers must be vigilant in making sure the tracking domain list is updated.[55]

C. Current Browser-Header Approach

This most recent idea, proposed by researchers at Stanford, is simpler and easier to execute than either of the previous approaches. In this approach, a user's browser sends a signal to a website that the user wants to opt-out of being tracked. It does so using an HTTP "header."[56] "Whenever a web browser requests content or sends data using HTTP, the protocol that underlies the web, it can optionally include extra information, called a 'header," explain the Stanford researchers.[57]

This mechanism "employs a decentralized design; it thus avoids the substantial technical and privacy challenges inherent to compiling, updating, and sharing a comprehensive registry of tracking services or web users."[58] Jonathan Mayer, one of the principal Stanford researchers, stated that while it operates differently, the Do Not Track registry, "much like the popular Do Not Call registry . . . provides users with a single, persistent setting to opt out of web tracking."[59]

Yet, in order to be effective, advertising companies will have to actually "listen" to this do not track signal being sent from users' browsers. According to the Stanford researchers, there are a variety of ways that this could be enforced, including self-regulation, "supervised self-regulation or 'co-regulation,' to direct regulation by an entity such as the FTC."[60] But based on our experience with the development of the Do Not Call registry and the practical problems that consumers face, it is EPIC's view that for a browser-based Do Not Track system to be successful, a centralized enforcement mechanism would be required.

---

[53] Ryan Singel, *supra* note 46.
[54] *Id.; see also* "Do Not Track Explained," *supra* note 45.
[55] "Do Not Track Explained," *supra* note 45.
[56] *Id.*
[57] "Do Not Track: Universal Web Tracking Opt-Out," project run by researchers at the Stanford Law School Center for Internet and Society and the Security laboratory at the Stanford Department of Computer Science, www.donottrackus.org
[58] *Id.*
[59] Cecilia Kang, "What a Do Not Track Option Might Look Like," The Washington Post Tech Blog, Nov. 17, 2010.
[60] "Do Not Track Explained," *supra* note 45.

The FTC recently released a privacy report that endorsed a Do Not Track mechanism but stopped short of discussing how such an approach would be made effective.[61] The report asks for comments on how Do Not Track would be implemented, but does explain that the most "practical method . . . would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits." The FTC report also states that "there must be an enforceable requirement that sites honor those choices" but is vague on the details of how such enforcement would occur.

In EPIC's view, the FTC discussion of the Do Not Track proposal should have paid much closer attention to the history of Do Not Call. The agency has, in effect, attempted to replicate a successful program, Do Not Call, without recognizing the steps that were required to make the program work.

IV. Issues with Do Not Track that Must Be Addressed

A. Opt-Out vs. Opt-In

Individuals' rights and privacy would be more effectively protected by an opt-in framework rather than the opt-out do not track list being considered. An opt-in approach would require online advertisers and tracking companies to obtain express consent before tracking individuals.

An opt-in framework would better protect individuals' rights and is consistent with most United States privacy laws. For instance, the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, Video Privacy Protection Act, Driver's Privacy Protection Act, and Children's Online Privacy Protection Act all empower the individual by specifying that affirmative consent is needed before information is employed for secondary purposes.[62]

Opt-in is more effective than opt-out because it encourages companies to explain the benefits of information sharing, and to eliminate barriers to exercising choice. Experience with opt-out has shown that companies tend to obfuscate the process of exercising choice, or that exemptions are created to make opt-out impossible. For instance, the Gramm-Leach-Bliley Act required opt-out notices to be sent to customers of banks, brokerage houses, and insurance companies.[63] These notices were confusing and incomprehensible to many Americans.[64] Opting-out often required the consumer to send

---

[61] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," Preliminary Federal Trade Commission Staff Report, p.66, December 2010, *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf.

[62] Respectively, at 20 U.S.C. § 1232g(b)(2)(A), 47 U.S.C. § 551(c)(2), 18 U.S.C. § 2511(2)(c), 18 U.S.C. § 2710(b)(2)(B), 18 U.S.C. § 2721(b)(11), and 15 U.S.C. § 6502(b)(A)(ii).

[63] 15 U.S.C. § 6801.

[64] Mark Hochhauser, "Lost in the Fine Print: Readability of Financial Privacy Notices," Privacy Rights Clearinghouse, July 2001*, available at* http://www.privacyrights.org/ar/GLB-reading.htm.

a separate letter to the company. Even if a consumer did opt out under the law, a company that wished to share consumer data could simply create a joint marketing agreement with another company to fall within an exemption to the prohibition on information sharing.[65]

In other contexts, phone companies have thwarted opt-out processes by demanding excessive authentication for opting out. For instance, the opt-out process for Customer Proprietary Network Information (CPNI) data sharing established by Verizon was confusing, and placed the burden on individuals to navigate a five-step process in order to opt-out.[66] Often, notices to consumers are not clear and therefore consumers are not making a meaningful choice when deciding whether to opt-out.[67]

While it seems that Do Not Track may end up being largely an opt-out type of mechanism, the idea that at least some data should be subject to consumers having to opt-in to have it collected should be considered, especially for sensitive health and financial information. If opt-out is the preferred strategy for Do Not Track, then it will require all of the elements that were eventually brought together for Do Not Call – centralized administration, enforceable legal protections, and a simple, transparent, and stable method for consumers to express their opt out preferences.

B. Opt-Out Cookies

It is also important that Do Not Track is not based on the idea of opt-out cookies, such as those advocated by the NAI.[68] Opt-out cookies have been used before as mechanism for consumers to opt-out of being tracked, but they have not generally been successful. Opt-out cookies are a confusing and misleading approach to consumer privacy. They are counter-intuitive, as users concerned with privacy typically delete cookies, especially those associated with search activities.[69] Yet once the cookie is deleted, the privacy setting is lost and advertisers will no longer honor the user's privacy status.[70] Second, the opt-out cookie does not scale. If users are required to accept opt-out cookies for every site that they do not want tracking them, a person would have to keep cookies for every single Internet site, which does not make sense.[71]

---

[65] 15 U.S.C. § 6802 (b)(2).
[66] *See* Letter from Marc Rotenberg, Executive Director, Electronic Privacy Information Center, to Ivan Seidenberg, President and co-CEO, Verizon (Feb. 7, 2002), *available at* http://www.epic.org/privacy/cpni/verizonletter.html.
[67] *See, e.g.,* FTC, "Transcript of December 7, 2009, Privacy Roundtable," Remarks of Alessandro Acquisti, Associate Professor, Carnegie Mellon University, Heinz College, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf ("However, I see notification, control, and transparency as necessary conditions, but insufficient. . . . There is by now a wealth of behavioral data and databases showing what are the gaps between what consumers want in terms of privacy and their ability to achieve these stated intentions.").
[68] *See, infra* p. 6.
[69] Letter from EPIC et al. to Jim Lanzone, CEO Ask.Com, Dec. 20, 2007.
[70] *Id.*
[71] *Id.*

The browser-header approach to Do Not Track seems to eliminate this concern, as it is not cookie-based, but rather browser-based.

C. What Information is Collected?

In any form of Do Not Track that it is implemented it is important to ensure that users are not required to give up private information in order to be on the registry or to use the browser-based mechanism. If an e-mail or IP address is collected, that could pose privacy concerns. Congress should investigate further what information the browser is sending back to companies in the "header" telling them that a user does not want to be tracked.

For example, the Ask Eraser product, which used opt-out cookies, inserted the exact time that a user enabled its product into the information that it sent in the browser.[72] The text string then operates like a unique identifier, such as a person's cellphone number or a social security number. While it is conceivable that there could be more than one cookie issued at the exact same second, it seems unlikely. Particularly, when histories are logged, reconstructing actual identity would be trivial. Also, even if Ask were not logging search histories, by transferring this type of cookie to third parties, it becomes easy for third parties to track users who have enabled Ask Eraser by simply noting the date/time stamp assigned.[73]

Therefore, any Do Not Track mechanism should be very cautious about what content is actually sent in the browser header to the online advertisers, and should ensure that it does not contain any information that can identify a user.

D. Tiered Web and Discrimination

The worst form of privacy discrimination is to make access to information conditional upon the relinquishment of personal information. There is a possibility that Do Not Track could lead to a tiered web, that is, one where those who use Do Not Track can only see certain content. Whether this will happen depends on how online advertisers react to Do Not Track, but there is some evidence to suggest that a tiered web will not necessarily result.

Currently, users can implement ad blocking through a browser plug-in, and many do, but very few sites refuse to provide content to users who have enabled ad blocking.[74] And ad blocking would be much more costly to advertisers as it prohibits all ads, as opposed to Do Not Track, which would only prevent behavioral ads.[75] Additionally, a tiered web already exists in the form of those who are logged in when they browse versus those who are anonymous. It is unlikely though that disabling Do Not Track as a

[72] *Id.*
[73] *Id.*
[74] "Do Not Track Explained," *supra* note 45
[75] *Id.*

requirement for service or access to content will ever become as popular as requiring log-in.[76]

Obviously this would be a major concern if those using Do Not Track are blocked from accessing web content. Part of the enforcement mechanism surrounding Do Not Track should include penalties for any websites that engage in this kind of discrimination.

E. Preemption

Congress should ensure that any Do Not Track legislation does not preempt state laws in the area of regulation of online data collection and targeted advertising. States have a traditional role in regulating privacy that should be preserved. There is a presumption in American law that state and local governments are primarily responsible for matters of health and safety.[77] Privacy is included in the category of health and safety issues, as an area of regulation historically left to the states.[78]

Federal consumer protection and privacy laws, as a general matter, operate as regulatory baselines and do not prevent states from enacting and enforcing stronger state statutes. The Electronic Communications Privacy Act,[79] the Cable Communications Privacy Act,[80] the Video Privacy Protection Act,[81] the Employee Polygraph Protection Act,[82] the Driver's Privacy Protection Act,[83] the Health Insurance Portability and Accountability Act,[84] the Gramm-Leach-Bliley Act,[85] and portions of the Fair Credit Reporting Act[86] all allow states to craft protections that exceed federal law. In each of the areas regulated by the above-referenced privacy laws, business has continued to flourish in states that have enacted privacy protections that are stronger than the federal law.

Permitting states to regulate interstate telemarketing will continue to promote regulatory innovation and experimentation. States enjoy a unique perspective that allows them to craft innovative programs to protect consumers. State legislators are closer to their constituents and the entities they regulate. Federal preemption can dilute more

---

[76] *Id.*
[77] *Hillsborough County v Automated Med. Labs*., 471 U.S. 707, 716 (1985) (there is a "presumption that state and local regulation of health and safety matters can constitutionally coexist with federal regulation).
[78] *See, e.g., Hill v. Colo.,* 530 U.S. 703 (2000) (upholding a law protecting the privacy and autonomy of individuals seeking medical care, as the law was intended to serve the "traditional exercise of the States' police power to protect the health and safety of their citizens." (internal quotation marks omitted).
[79] 18 U.S.C. § 2710(f)(2005)
[80] 47 U.S.C. § 551(g) (2005)
[81] 18 U.S.C. § 2710(f) (2005).
[82] 29 U.S.C. § 2009 (2005).
[83] 18 U.S.C. § 2721 (2005)
[84] 29 U.S.C. § 191 (2005)
[85] 15 U.S.C. § 6701 (2005)
[86] 15 U.S.C. § 1681t (2005).

vigorous protections and policy debates that occur at the state level. For example, in a detailed study of caller ID policy approaches, researchers found that the FCC's position was much weaker than those developed by the states.[87] State and local governments are also more accountable than the federal government to their constituents. As a result, it is likely that stronger protections will emerge and more vigorous enforcement will be pursued by state actors.

Businesses are not put at a disadvantage by having to comply with differing state laws. In fact, businesses have long accommodated themselves to a range of state consumer protection statutes while maintaining a profitable enterprise. Courts have, for years, engaged in a process of reconciling potentially or actually conflicting laws through application of established legal principles to various factual situations. Such a tailored response is especially appropriate with respect to evolving technologies and new applications of those technologies. This flexible approach accommodates the needs of both businesses and consumes, while preserving state sovereignty in an area where states have traditionally had a significant role.[88]

F. Enforcement

As discussed earlier, this Do Not Track mechanism would need to be enforced by an agency such as the FTC.[89] And the enforcement must have teeth, otherwise it will not be at all effective. In addition to meaningful oversight by a federal agency, there should also be a private right of action that gives individuals, whose rights have been violated, the opportunity to seek relief. A private right of action is necessary even where a federal agency is given enforcement authority. Agency action is always discretionary and there is no guarantee, absent a private right of action, that an individual whose rights may have been violated will have the opportunity for relief. This problem has become even more evident in the least few years with the spotty record of the current FTC on matters concerning the protection of consumer privacy.

V. Conclusion

Online data collected and targeted behavioral advertising pose a serious threat to consumer privacy. A Do Not Track mechanism, while important, only starts to solve one of the many problems with online data collection. EPIC respectfully requests the Committee to fully consider all of the issues with Do Not Track outlined in this statement, as well as the relevant history of the TCPA and Do Not Call list. A Do Not Track list can be an important tool, but only if it is done thoughtfully and enforced fully. At a minimum, EPIC believes that key to an effective Do Not Track technique will be the adoption of legislation that makes the decision by consumers enforceable, stable, transparent, and simple.

---

[87] Comments of EPIC et all to FCC regarding "Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991," July 29, 2005, at 9.

[88] *See, e.g.,* The national Association of Attorneys General Privacy Subcommittee, "Privacy Principles and Background," *available at* ihttp://www.naag.org/naag/resolutions/subreport.php.

[89] *See supra* Part III.C

We would also strongly urge the Committee to undertake a more thorough examination of the Commission's strategy for safeguarding consumer privacy. In many areas, we believe the FTC has failed to take necessary steps to address clear public concerns about the collection and use of personal data for commercial purposes.

Thank you for your consideration of these views.