Daniel D. Castro
Senior Analyst
Information Technology and Innovation Foundation

"Do-Not-Track" Legislation: Is Now The Right Time?

Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

December 2, 2010

Mr. Chairman and members of the Committee, I appreciate the opportunity to appear before you to discuss the implications of "Do Not Track" legislation for the Internet. My name is Daniel Castro. I am a senior analyst at the Information Technology and Innovation Foundation (ITIF) and a former IT auditor at the Government Accountability Office. ITIF is a nonpartisan research and educational institute whose mission is to formulate and promote public policies to advance technological innovation and productivity.

Privacy concerns associated with information technology (IT) and the Internet must be taken seriously, but it is important to keep a sense of perspective. Historically, major new technologies have prompted what in hindsight were overblown privacy fears. To cite an example, some people objected to easy-to-use cameras, fearing that an individual's activities would no longer be private when walking down the street.[1] Or to cite another example, when transistors were first developed, there was a short-lived privacy scare that everyone would be able to be snooped on using small electronic "bugs." In fact, a *Life Magazine* cover story trumpeted "Insidious Invasions of Privacy" and Congress even went so far as to hold hearings on the matter.[2] Of course, all this fuss was much ado about very little.

Society has always learned to manage these so-called threats in large part because of the fact that many—but certainly not all—of the concerns raised by privacy activists then as well as now are hypothetical and speculative.[3] Given the large amount of information in digital format today, it is worth asking how much harm has been done to date. Notwithstanding all the fear and gloom from privacy activists, there simply have not been widespread privacy violations caused by existing privacy laws and regulations. Moreover, the debate on privacy to date has been driven largely by privacy fundamentalists (i.e., those individuals who value personal privacy above all other values) that advocate protecting individual privacy above all else, no matter the costs or consequences. However, as with most issues, policymakers should take a balanced approach that

considers both the needs of individuals and the impact on society, rather than focusing exclusively on the demands of individuals that come at the expense of the collective good.

Online advertising is a crucial part of the Internet ecosystem, but unfortunately it has been misunderstood by some. For the last few years privacy fundamentalists have called for a national Do Not Track feature for online activity modeled after the national Do Not Call Registry managed by the Federal Trade Commission (FTC). 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 that would ultimately be borne by consumers, 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 content and fewer free services online. In short, a Do Not Track requirement would do more harm than good and for that reason ITIF urges the federal government to not go forward with this approach.

Online Advertising Benefits Consumers

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[4]), and online advertising is the fuel powering this economic dynamo.[5] ITIF estimates that the annual global economic benefits of the commercial Internet equal $1.5 trillion, more than the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.[6] 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.

As shown in Figure 1, Internet advertising has grown dramatically over the past decade. In the United States, non-search online advertising expenditures have grown from $6 billion in 2002 to $13 billion in 2007. Similarly paid search has grown from $1 billion in 2002 to $8 billion in 2007.[7] The Internet Advertising Bureau estimates the cumulative U.S. Internet online advertising market to be $22.7 billion as of 2009.[8] The Kelsey Group found that worldwide Internet advertising reached approximately $45 billion in 2007, out of a total $600 billion advertising market, and predicts online advertising will grow to over $147 billion by 2012.[9] IDC reports similar figures estimating that worldwide spending on Internet advertising reached $61 billion in 2009. In addition, IDC predicts that advertisers will increasingly use the Internet for advertising, with online ad spending growing from 10 percent of all ad spending in 2009 to almost 15 percent by 2013.[10]

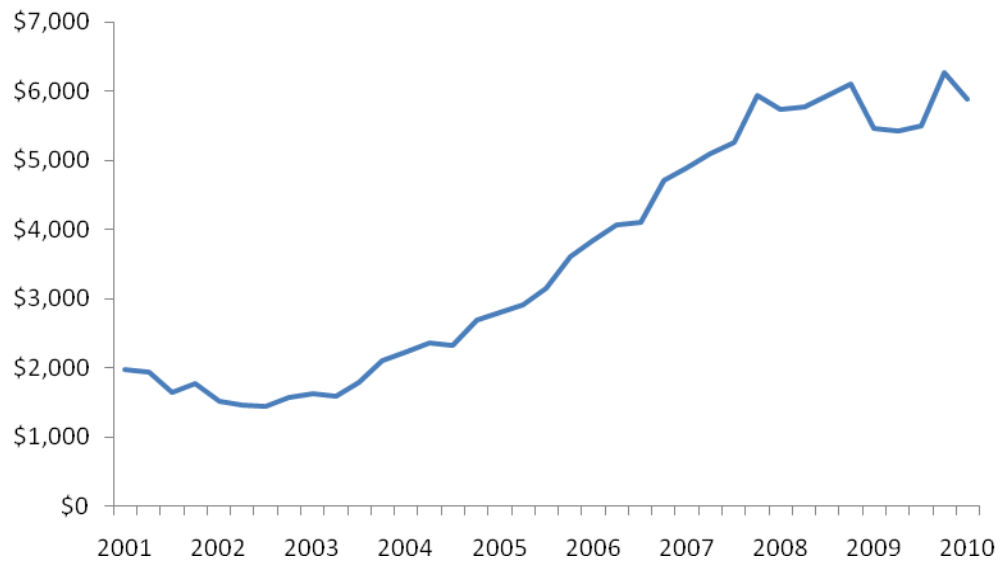

Figure 1: U.S. Quarterly Internet Ad Revenue since 2001, Source: IAB/PWC[11]

Internet advertising supports the creation and maintenance of new online content, applications and services including news, videos, music, games, social networking, reference, email and other online services. Indeed, many of the websites that millions of Americans use daily for work and play would not be around today without online advertising. In fact, of the top five most popular websites in the United States—Google, Facebook, Yahoo, and YouTube all use online advertising almost exclusively to support their products and services and Amazon.com uses it to supplement theirs.

In particular, online advertising benefits online publishers like news outlets. Policymakers concerned with the decline of print media should note that greater revenue from targeted online advertising will likely be necessary for journalism to survive in the Internet age.[12] We are already seeing some evidence of this. For example, the Los Angeles Times announced in 2009 that its online advertising revenue was sufficient to cover its entire editorial payroll.[13] And online advertising will be important for the so-called "long tail" of small websites and content producers supported by ad revenues. After Google introduced a revenue-sharing program in 2007 for YouTube, various Internet entrepreneurs began turning their videos into a lucrative business. For example, Josh Chomik, a teenager in New Jersey earns around $1,000 a month from ad revenue generated by his YouTube videos.[14]

Consumers download many different types of applications supported by online advertising. These include products from major U.S. technology companies like Google and Microsoft. For example, Google Apps, which includes free Internet-based applications for word processing and email, is funded by online advertising. Similarly Microsoft Office Live is available in a no-cost, ad-supported version and Microsoft Office Starter 2010, a reduced-functionality version of

Microsoft Office which includes display advertising, is available to consumers for free. Fast-growing start-ups like Evernote which has over 5 million users offers both an online application and a desktop application for taking notes at no cost with advertising. IT professionals routinely use free, ad-supported software like Spiceworks to monitor and manage their networks. Even the fast-growing health IT field has advertising-based products: Practice Fusion is a no-cost, web-based electronic health record solution for doctors.[15] Rather than charge doctors a monthly fee, the hosted service is provided for no charge to doctors who use the ad-supported service. Alternatively, health care providers can pay a $100 per month to access the service without ads.

If online advertising is central to the health of the U.S. Internet ecosystem today, then ensuring that online advertising revenue continues to grow will be central to the Internet's growth and success tomorrow. One key way websites gain more value from online advertising is by providing more relevant ads—a benefit both to consumers who get more utility from these ads and advertisers who are willing to pay more to reach their target audience. Targeted ads based on information about a user—such as the user's browsing history or other user-specific data—help deliver higher-value ads. Many of these ads can be delivered using non-personally identifiable information since the interests of the user often do not need to be tied to an actual identity.

Targeted advertisements are more effective than non-targeted online ads since they are more relevant to users' interests. Click-through-ratios, or the percent of Internet users that click on an ad, are as much as 670 percent higher for targeted ads than non-targeted ads.[16] These ads also generate more revenue. Advertising rates for online ads that use behavioral targeting are significantly higher than online advertising that do not use behavioral targeting (one study found it to be 2.68 times as much).[17] Moreover, 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. Yet even though the importance of online advertising to the greater Internet economy and American consumers has been well-documented, some advocates and policymakers seem intent on imposing data privacy regulations that would limit the ability of Internet publishers to tailor advertising to users based on their interests.

Part of this may be due to a misconception about how targeted advertising works. When Google first offered ads to users of its free Gmail service based on contextual information in emails, privacy advocates objected to Google "reading people's email."[18] Yet these claims do not distinguish between ads delivered to Internet users through automated computer technology and an individual snooping through a person's emails. In the former, providing targeted computer-matched ads poses no more privacy threat to users than simply having their emails stored on remote servers because there is no additional information to which Google has access.

Similarly privacy concerns have been raised about online advertisers like Facebook with fictional claims of the company selling its user's data because of misunderstandings about the mechanisms of targeted advertising. Targeted advertising works by matching ads to users based

on the information in their profile. For example, a wedding photographer in Dallas can pay Facebook to serve an ad to everyone in Dallas who switches their relationship from “single” to “engaged.” This benefits everyone—the photographer gets more clients, the users get more relevant ads, and Facebook is better able to fund its free services. But at no time does the photographer learn who sees the ads, unless a user chooses to make contact.

Web-Based Tracking Used For More Than Just Online Advertising

Like online advertising, Internet-based “tracking” is also misunderstood. One problem with the term “tracking” is that it is an overly-broad term that does not correlate to a specific technical activity. Many activities could be considered tracking: setting unique identifiers for users in their web browser cookies, logging IP addresses on a server, monitoring IP packets over a network, and building unique profiles for users on a website. Policymakers should remember that companies collect data for many purposes besides providing targeted advertising. Google, for example, uses data provided by consumers for everything from tweaking its search results to developing its free email service to improving its speech-to-text engine that is now used on mobile phones. Many websites use consumer data to deliver personalized services to deliver content to users based on information they, or a third party, know about the user. Online newspapers like the Washington Post use information provided by social networks to display articles recommended by a user’s friends. The online music service Pandora can use information from an individual’s Facebook profile (with the user’s permission) to create a customized web-based radio station tailored to that user’s musical preferences. Even when used for online advertising, companies do not just collect data to deliver customized user ads. Online advertisers use logs, for example, to create an audit trail so that they can prove to their customers that they have delivered the number of ads that they have sold and prevent criminal activity, including click fraud.

When privacy activists refer to online tracking they are most commonly referring to cookie-based tracking of users. Many websites use HTTP cookies—small data files stored on a user's computer by a web browser. When a user visits a website, the website can request that the user’s web browser store certain data in a cookie. By default, most web browsers allow this activity. A cookie may be used to store temporary data, such as the contents of a shopping cart for e-commerce, or to remember a user on subsequent visits to the website, such as for customizing a website. Each cookie is accessible only by the Internet domain that created the data.[19]

For many privacy activists the risk from cookies is as follows: under some circumstances, cookies can be used to help website operators track website usage over time and build a profile of the activity of an instance of a web browser with the cookies on it (which may or may not tie back to a specific user). This profile can then be used to deliver targeted ads to a user based on his or her interests, such as travel or sports. In addition, if the website collects personally identifiable information, the website operator could link some browsing activity to individual identities instead of just the computer or browser being used. This could potentially lead to the

intentional or accidental disclosure of an individual's web browsing history—a clear violation of a user's expected level of privacy. Privacy advocates see the collection and misuse of such data to be the primary threat of cookies.

However, cookies also offer many benefits to consumers. Website developers use cookies to create robust online applications that offer a better user experience. Perhaps the most common use of cookies is to facilitate online commerce. Online shopping cart applications routinely use cookies to maintain the list of which items a shopper wants to purchase. In addition, if the user accidentally closes the web browser or the browser crashes, the user can often return to the website without having to reload items back into the shopping cart. Cookies facilitate these functions transparently to the user. Cookies also enable users to customize websites. For example, users can personalize settings such as preferred language or region so the website will recognize their preferences on subsequent visits. Weather.com uses cookies to remember a returning user's zip code and automatically displays the weather report for that user's geographic area. For websites requiring a login, cookies can be used to authenticate users so that the user does not have to always enter a username and password to access a website. Website operators also use cookies to learn how to best engage with their audience and measure the success of online content and online advertising. Cookies help website developers produce more advanced website analytics to better understand how users interact with their website. For example, cookies allow website developers to learn how many of their visitors are new or returning users.

Cookies can be classified based on the source of the cookie and the lifespan of the cookie. When classified by the source, cookies come in two flavors: first-party cookies and third-party cookies. First-party cookies refer to cookies created by the domain of the website that the user entered in the web browser. Third-party cookies are those created by affiliated domains, such as advertising networks used by the primary website visited by the user. For example, a user that visits CNN.com not only will receive cookies for CNN.com, but also for other domains used by online advertisers employed by CNN, such as doubleclick.net, revsci.net, and questionmarket.com.[20] Advertisers can use third-party cookies to track user preferences across multiple websites for targeted advertising. All major web browsers include the option to block third-party cookies.

When classified by lifespan, there are two types of cookies: session cookies and persistent cookies. Session cookies, as the name implies, last only as long as the user is on a particular website. Session cookies enable websites to remember data about users as they navigate from page to page on the same website.[21] For example, session cookies enable technologies like online shopping carts. Persistent cookies last beyond the initial web browsing session. The cookies can be set to expire at a certain time or last indefinitely.[22] These types of cookies are useful so that a website can recognize a returning user. For example, a website can use a persistent cookie to recognize a user on return visits, thus saving the user from having to log in at every visit.

Why Do Not Track Would Not Work

While the Do Not Track proposal is not new, it has received renewed attention in recent months. FTC chairman Jon Leibowitz testified in front of Congress 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.[23] 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.

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.[24] 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.[25] This implementation of Do Not Track would also likely not apply to other emerging forms of online advertising such as that provided by Phorm or the now defunct NebuAd which uses deep packet inspection to deliver targeted advertising in coordination with ISPs. Policymakers should be careful not to devise policies around a particular business model that would end up harming some businesses and business models while helping others.

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 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.[26]

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 professors 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.[27]

The federal government would also not be able to effectively enforce a Do Not Track proposal. While it is easy to determine if someone violates a Do Not Call list, it is significantly more difficult to determine if someone is violating a requirement not to record certain data about users as they visit a website. 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 standards bodies. Would U.S. consumers be stopped from downloading browsers made in other nations that are not covered by this regulation?

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.[28] 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 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 telephone company said in exchange for free telephone service marketers get to call your phone 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. So it makes sense to have an easy-to-use opt out system for unsolicited telephone calls.

In contrast, Do Not Track is like getting the free telephone service without taking the marketing 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, some consumers are trying to get something for nothing.

This is essentially a case of the famous prisoner's dilemma. If no one opts out of targeted advertising, the overall Internet ecosystem continues to grow and consumers continue to benefit through the creation of more free content, applications and services. If one person opts out, but other users do not, the overall value of the Internet ecosystem diminishes by a very small amount. But if everyone, or a large share of Internet users, opts out, then the overall value of the Internet ecosystem diminishes by a significant degree. In this case, what may appear to be rational for the individual is irrational and destructive to society. The last thing government should be doing is making it easier for individuals to act in a way that is harmful to society.

This is not to say that consumers should not be able to avoid targeted advertising. But the way to do that is to not access sites that display this type of advertising and use existing tools to manage online privacy. But 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 activists pushing for Do Not Track want to have their cake and eat it too. If the marketplace could evolve 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.[29] They might even call for public funding of Internet content so that users would not have to see advertising.

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.

Policymakers Should Avoid Policies That Would Halt Innovation Online

The Internet is a vital part of economic and social life and policymakers must be vigilant against expensive and ineffective policies that would curtail beneficial uses of data. Congress should not implement heavy-handed privacy regulations without seeking a better understanding of how these changes will affect the Internet economy, and by extension, the overall economy and society. A recent example in Europe shows that the impact of these policies is not always evident at the outset. As discussed above, Goldfarb and Tucker analyzed the impact of the European Union's Privacy and Electronic Communications Directive (2002/58/EC) which was implemented in various European countries and limits the ability of advertisers to collect and use information about consumers for targeted advertising. The authors find that after the new privacy laws went into effect they resulted in an average reduction in the effectiveness of the online ads by approximately 65 percent (where the effectiveness being measured is the frequency of changing consumers' stated purchase intent). The authors write "the empirical findings of this paper suggest that even moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all websites, and that the costs should be weighed against the benefits to consumers."

Targeted advertising is crucial for supporting the websites responsible for the majority of the free and low-cost content online. This is particularly true for general-interest sites (like news websites) that have little ability to determine what ads their users would be most interested in without the cues that better targeting enables (in contrast to some special-interest sites which can do so somewhat more easily). Not surprisingly, Goldfarb and Tucker found that the negative impact on ad effectiveness from the European privacy regulations was strongest among these sites. The negative impact was also stronger for non-obtrusive ads (e.g. smaller ads or ads not using multimedia) which suggests that small, text ads will be significantly less effective unless they can be tailored to a user's interests. The authors also note that if European advertisers reduced their spending on online advertising in line with the reduction in effectiveness resulting from stricter privacy regulations, "revenue for online display advertising could fall by more than half from $8 billion to $2.8 billion."[30] And as Beales notes, a reduction in ad revenue directly hurts online publishers since more than half of ad network revenue goes to publishers who host the ads.[31]

It is therefore not surprising that U.S. Internet companies lead the world and European companies do not.[32] European companies are at a disadvantage compared to U.S. companies because the government is essentially limiting their revenue to less than half of what they could otherwise earn. As a result, Europe has struggled to be an effective player in the Internet economy compared to the United States where there are significantly fewer restrictions.

As ITIF has noted, proposed privacy regulations in the United States would restrict targeted online advertising by limiting the collection of certain types of data, requiring opt-in consent for collecting data, or providing mechanisms to encourage users to opt-out of targeted ads.[33] Like the European privacy regulations, these types of restrictions would limit targeted advertising and harm the Internet-powered economy. These kinds of privacy regulation would reduce revenue flowing into the U.S. Internet ecosystem, which means not only fewer websites and less valuable content, but also less spending by Internet companies on servers and bandwidth. The net result will be fewer jobs. In addition, if the Internet is less valuable to consumers because there is less useful content, applications and services, users are less likely to subscribe to broadband.

Does this mean that policymakers should avoid all privacy regulations? Of course not. But it does suggest that policymakers should tread lightly and focus more on preventing harms from privacy violations than on legislating expensive and revenue-reducing regulations.[34] The evidence clearly suggests that the tradeoffs of stronger privacy laws result in less free and low-cost content and more spam (i.e. unwanted ads) which is not in the interests of most consumers.

Proponents of stricter privacy laws often ignore the benefits that online advertising confers on consumers. For example, Google and Facebook, two of the companies most vilified by privacy fundamentalists, are at the forefront of offering low or no-cost content, applications and services to consumers unimaginable a decade ago. Yet when these companies use targeted online advertising to fund their operations, privacy fundamentalists object. Unfortunately, these objections reflect the prevailing message of privacy fundamentalists that privacy trumps all other values. However, policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can, as it will here, come at a real financial cost—fewer jobs, less investment, and less free content for users.

Current Privacy Tools Provide Consumers Various Means of Managing Their Privacy

Consumers today have many different options for controlling their online privacy that are more cost-effective than the Do Not Track proposal. Every major web browser includes many features to allow users to manage their online privacy settings, such as the use of cookies, and this is a continued source of innovation and differentiation among competing web browsers. Consumers can also download third-party web browser plug-ins like AdBlock and NoScript which block online advertising. Internet users can also use new applications like Bynamite which provide individuals a third-party interface to the profiles maintained about users by online advertisers and allows users to change, delete or add to their list of interests for targeted online advertising (e.g. a user could specify that they are interested in receiving ads for the categories “politics” and “education” but not “cooking”).

Online advertisers are developing industry best practices to provide consumers with transparency and choice when using sites with targeted advertising. The Digital Advertising Alliance, an industry coalition, has created a self-regulatory program for online behavioral advertising, a

unique icon so consumers can identify interest-based ads, and an online tool to allow consumers to select their advertising preference for over 50 participating ad networks.[35] Individual ad networks have also created their own tools to allow users to manage their advertising preferences. For example, Google, a major online ad network, allows users to opt-out of targeted advertising using the DoubleClick cookie or through an optional opt-out plug-in for their web browser (the plug-in is available for Chrome, Firefox and Internet Explorer). Many third-party online advertisers, such as those belonging to the Network Advertising Initiative have also made a similar opt-out tool available online for users to more easily avoid targeted online advertising.[36] In other words, citizens increasingly have tools to ensure that online interactions occur on their own terms. And for the relatively small share of Americans who want to consume free Internet services while not allowing themselves to be served more relevant ads, these options for them to opt-out are sufficient.

Policymakers Should Pursue Privacy Policies That Foster Innovation

Do Not Track is an attempt by privacy fundamentalists to stop 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.[37] 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. Consumers ultimately care about how their data is used, not whether data is obtained by tracking Internet usage, consumer sales data or information that an individual discloses on a social networking site. 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. Targeted advertising, like any other technology, will improve over time and it would be a mistake to halt the progress of such a promising innovation.

Conclusion

As data on individuals and their actions increasingly is collected and stored electronically, it is important for policymakers to consider the effect this has on privacy. This hearing provides a welcome opportunity to explore the best ways of protecting individual privacy while avoiding constraints on business innovation and unintended negative impacts on the economy, U.S. competitiveness, and consumers. Do Not Track would not be an effective tool to achieve this end because of its significant costs and shortcomings. Privacy is important, but it must be balanced against competing goals including usability, cost, future innovation and consumer benefits.

Notes

1. For a modern day example of misplaced privacy fears, see Daniel Castro, "I Spy a Luddite: Why the Lawsuit over Google Street View is Absurd," Information Technology and Innovation Foundation, Washington, D.C., April 25, 2008, http://www.itif.org/files/WM-2008-03.pdf.
2. John Neary, "Electronic Snooping—Insidious Invasions of Privacy," *Life Magazine,* May 20, 1966. http://www.bugsweeps.com/info/life_article.html.
3. Robert D. Atkinson, "RFID: There's Nothing to Fear Except Fear Itself," remarks at the 16th Annual Computer, Freedom and Privacy Conference, Washington, D.C., May 4, 2006, http://www.itif.org/files/rfid.pdf.
4. 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.
5. 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.
6. Robert Atkinson et al., "The Internet Economy 25 Years After .com," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http:// www.itif.org/files/2010-25-years.pdf.
7. 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.
8. "IAB Internet Advertising Revenue Report," IAB, April 2010, http://www.iab.net/media/file/IAB-Ad-Revenue-Full-Year-2009.pdf.
9. "Interactive Advertising Revenues to Reach US$147 Billion Globally by 2012, According to The Kelsey Group's Annual Forecast," press release, (Chantilly, VA: The Kelsey Group, 2008), http://www.kelseygroup.com/press/pr080225.asp.
10. "Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013, According to IDC," IDC, press release, December 9, 2009, http://www.idc.com/getdoc.jsp?containerId=prUS22110509.
11. "Internet Advertising Revenues Hit $5.9 Billion in Q1 '10, Highest First-Quarter Revenue Level On Record," IAB, May 13, 2010, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-051310.
12. Robert D. Atkinson, "Federal Trade Commission Workshop on Journalism in the Digital Age," (Washington, D.C.: Information Technology and Innovation Foundation, 2010) http://www.itif.org/publications/federal-trade-commission-workshop-journalism-digital-age.
13. Jeff Jarvis, "History in the making in LA as online ads hit target," The Guardian [UK] 12 Jan. 2009, http://www.guardian.co.uk/media/2009/jan/12/la-times-online-advertising.
14. "YouTube channel earns college money for N.J. teen," NJ.com, 7 April 2009, http://www.nj.com/news/index.ssf/2009/04/youtube_channel_earns_college.html.
15. "Free Electronic Medical Record (EMR)," Practice Fusion, n.d., http://www.practicefusion.com/pages/free_ehr.html.

16. Jun Yan, Gang Wang, En Zhang, Yun Jiang, & Zheng Chen, "How Much Can Behavioral Targeting Help Online Advertising?" (Madrid, Spain: WWW, 2009), http://www2009.eprints.org/27/1/p261.pdf.
17. Howard Beales, "The Value of Behavioral Targeting," 2009, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
18. Robert Atkinson, "Google E-mail, What's All the Fuss About?" (Washington, D.C.: Progressive Policy Institute, 2004) http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=288&contentID=252511.
19. Other similar technologies, such as web beacons (AKA "web bugs" or "tracking pixels") and Flash cookies (AKA "local shared objects") have also been criticized by some privacy advocates.
20. Data from author experiments on May 11, 2009.
21. Cookies enable a stateful web browsing experiences over HTTP—a stateless protocol.
22. Technically the cookie has an expiration date, but this can be set to a date beyond the expected lifespan of the computer.
23. 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.
24. "Operation of the Do Not Track List," Center for Democracy and Technology, October 31, 2007, http://www.cdt.org/privacy/20071031donottrack.pdf.
25. 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.
26. 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.
27. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
28. 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.
29. A sample post along these lines can be found here: http://activerhetoric.wordpress.com/2010/11/08/do-not-track-means-do-not-track/
30. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
31. Howard Beales, "The Value of Behavioral Targeting," 2009, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
32. Robert D. Atkinson, Stephen J. Ezell, Scott M. Andes, Daniel Castro, and Richard Bennett, "The Internet Economy 25 Years After .com," Information Technology and Innovation Foundation, March 15, 2010, http://www.itif.org/files/2010-25-years.pdf.
33. Daniel Castro, "ITIF Comments on Draft Privacy Legislation," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http://www.itif.org/files/2010-privacy-legislation-comments.pdf.
34. Daniel Castro, "Data Privacy Principles for Spurring Innovation," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http://www.itif.org/files/2010-privacy-and-innovation.pdf.
35. "Opt Out From Online Behavioral Advertising (BETA),"Digital Advertising Alliance, n.d., http://www.aboutads.info/choices/ (accessed On November 29, 2010).
36. "Opt Out of Behavioral Advertising" Network Advertising Initiative (NAI), http://www.networkadvertising.org/managing/opt_out.asp (accessed May 11, 2009).
37. "Online Behavioral Tracking and Targeting: Legislative Primer September 2009," Center for Digital Democracy, September 2, 2009, http://www.democraticmedia.org/doc/privacy-legislative-primer.