INTERNET TRACKING: STALKING OR A NECESSARY TOOL FOR KEEPING THE INTERNET FREE?

Wesley Gee†

“There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”

I. INTRODUCTION

Imagining the world George Orwell brought to life in his seminal novel 1984 is almost impossible. As Americans, we have come to expect a certain amount of privacy in our daily lives. We trust that information like our age, where we live, and the identities of our relatives will stay personal, as long as we keep it so. We shop, dine, and travel without inhibition, believing that our daily activities will go unnoticed by the masses. If someone were to follow our every move, we would resort to the law and file charges for stalking.² Most people, therefore, would be alarmed to find that their information and behavior is tracked and compiled on a daily basis—online. Congress’ lack of action has

---

† J.D. Candidate, May 2012, The Catholic University of America, Columbus School of Law. Wesley wishes to express gratitude to his parents and family for their unending love and support. Thanks also to Maureen Ohlhausen for providing expert advice and the CommLaw Conspectus staff for their patience and hard work throughout the writing process.


2 See, e.g., D.C. CODE § 22-3133 (2001); MD CODE ANN., CRIM. LAW §§ 3-801, 802 (West 2004); VA. CODE ANN. § 18.2-60.3 (2002); 18 PA. CONS. STAT. § 2709.1 (2003); DE L. CODE ANN. tit. 11, § 1312 (2007).
allowed Internet sites are allowed to engage in such behavior every day.  

Internet advertising is now a $26 billion per year industry, up from just under $5 billion in 1999. The industry has become so lucrative that in 2007, Google, Yahoo, Microsoft, and AOL all purchased major Internet advertising companies for billions of dollars. This is largely because Internet advertising companies now use a method known as “behavioral advertising,” which uses vast amounts of personal data collected by tracking users’ online behavior in order to specifically tailor advertisements to these individuals. Behavioral advertising has become so prevalent that a recent Wall Street Journal study found that the 50 most-visited Web sites by Americans, on average, “installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning. A dozen sites each installed more than a hundred.”

However, Americans are becoming increasingly concerned about their privacy online. In July 2010, a study found that 90% of those polled wanted more legal protection for personal information, with 84% in favor of requiring companies to obtain explicit approval to track personal information. Moreover, a December 2010 USA Today/Gallup poll found that 67% of Internet users in the U.S. felt that advertisers should not be allowed to track online activity in order to target specific ads to individual users. Additionally,

---

3 In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001). A class action suit was brought against DoubleClick alleging that their storage and use of cookies to target Internet advertisements at users violated the Electronic Communications Privacy Act, Federal Wiretap Act, Computer Fraud and Abuse Act, and state law. Id. at 499-500. The court found that plaintiffs failed “to plead violations of any of the three federal statutes under which they bring suit. The absence of evidence in the legislative or judicial history of any of these Acts to suggest that Congress intended to prohibit conduct like DoubleClick’s supports this conclusion.” Id. at 526.


6 Simson Garfinkel, How to Stop the Snoopers, MIT TECH. REV. (Mar./Apr. 2011), http://commcns.org/ru20f8 (explaining that behavioral advertising works by downloading tracking technology onto computers when users visit Web sites, which relays information about the users Internet surfing habits to advertisers).

7 Julia Angwin, The Web’s New Gold Mine: Your Secrets, WALL ST. J. (July 30, 2010), http://commcns.org/uw4Dqc (asserting that so much information is now available that a secondary industry of “data brokers” has emerged to compile this data into profiles and sell it to advertising companies for one tenth of a penny).


9 Id.

61% of respondents believed that these methods were not justified to keep costs for content low or free.\footnote{11}

Responding to Internet privacy concerns, the Federal Trade Commission ("FTC") proposed a new framework to govern Internet tracking in a preliminary report released in December 2010 ("FTC 2010 Report").\footnote{12} The centerpiece of the framework, a "Do Not Track" mechanism, would allow Internet users to opt out of being tracked online.\footnote{13} However, while the FTC asked for public comment on the proposed framework, Commissioner J. Thomas Rosch stressed that the FTC was not endorsing a "Do Not Track" mechanism.\footnote{14} Members of Congress also attempted to address concerns about online tracking in 2011. Senator John D. Rockefeller and Congresswoman Jackie Speier introduced separate pieces of legislation directing the FTC to establish requirements for a "Do Not Track" mechanism.\footnote{15} Congressman Bobby Rush and Senators John McCain and John Kerry introduced separate bills addressing Internet privacy.\footnote{16} While neither of these bills mandated a "Do Not Track" mechanism, they both require the FTC to develop a more comprehensive framework to address Internet privacy.\footnote{17}

Part II of this Comment provides further background on Internet tracking and advertising, while examining the benefits and harms of such data collection. It goes on to discuss the history of the FTC’s regulatory oversight regarding privacy issues in Part III, in addition to scrutinizing the agency’s proposed framework. Part IV analyzes the separate pieces of legislation proposed by Reps. Jackie Speier and Bobby Rush, ultimately noting that Rep. Rush’s approach more effectively balances the data collection practices necessary for the Internet to function efficiently with consumer privacy.

\footnote{11}{Id.}
\footnote{12}{See FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT 39-68 (2010) [hereinafter FTC 2010 REPORT].}
\footnote{13}{See id. at 63-69.}
\footnote{14}{J. Thomas Rosch, The Dissent: Why One FTC Commissioner Thinks Do Not Track is Off-Track, ADVERTISING AGE (Mar. 24, 2011), http://commcns.org/vjrWGg.}
\footnote{15}{See Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011).}
\footnote{16}{See Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (Best Practices) Act, H.R. 611, 112th Cong. (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011). Congressman Cliff Stearns also introduced a bill addressing Internet privacy without a Do Not Track mechanism mandate. See Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011). This bill is significantly less comprehensive than either of the other two pieces of legislation and will not be discussed in this comment.}
\footnote{17}{See Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (Best Practices) Act, H.R. 611, 112th Cong. (2011).}

II. INTERNET TRACKING AND BEHAVIORAL ADVERTISING: WHAT IS IT AND HOW DOES IT AFFECT ME?

Prior to the advent of tracking and behavioral advertising, Internet advertisers simply purchased ad space on a particular Web site, similar to newspaper advertisements. Advertisers bought ads “based on proximity to content”—a sports retailer might buy ad space on a sports news site or a university might buy ad space on a college-ranking site. However, new tracking technology enables advertisers to target specific advertisements at specific customers by “paying a premium to follow people around on the Internet.” Companies use this information not because they are against privacy, but because the personal information collected from tracking enables them to better tailor advertising and increase revenues.

A. The Mechanics of Internet Tracking

Companies use two main methods to track users. One such method is to track a user’s search history through his or her Internet Protocol Address. Another method involves placing a small file on a user’s computer to monitor the Web sites the user visits, as well as his or her preferences for the particular Web site. While these practices may be necessary for the Internet to function efficiently, they can pose significant privacy issues for individual users.

I. Search Based Tracking and Advertising

Every computer connected to the Internet is assigned a unique Internet Protocol (“IP”) address that it transmits to any Web site it visits. Since most

---

18 Angwin, supra note 7.
19 See id.
20 Id.
22 See infra Part II.A.1.
23 See discussion, infra Part II.A.2.
24 See discussion, infra Parts II.A.1-2.
25 Each computer on the Internet has a unique IP address, a 32-bit binary number, which consists of a string of 32 ones or zeros. This long binary number, in base 2, can be sectioned off into four bytes, each eight bits long. In turn, each byte can be converted into a number in base 10 ranging from 0-255. Thus, all IP addresses can be represented as #.#.#.#, where each ‘#’ is a number from 0-255. This representation is sometimes called a ‘dotted quad.’
people have used a search engine\textsuperscript{27} such as Google, Yahoo, or Bing, pulling up any recent Internet history might uncover searches for information on medical problems, dating services, clothing stores, and a multitude of other information consumers may want to keep private.\textsuperscript{28} Some search engines store this data, as well as every query a user makes, in a database for extended periods of time.\textsuperscript{29} All queries from a single IP address are then compiled to create a detailed profile of an individual’s “interests, political views, medical conditions, wishes, and fears.”\textsuperscript{30} This enables companies to target advertisements to specific IP addresses or sell advertisement space to companies that may appeal to the individual behind the IP profile.\textsuperscript{31}

In an attempt to allay privacy concerns, search engines anonymize the queries by not linking any user identities to their searches or profiles.\textsuperscript{32} However, this has proved to be an inadequate protection.\textsuperscript{33} In 2006, AOL accidentally released a database matching 657,000 users, identified by numbers, with the 20 million web searches made over a three-month period.\textsuperscript{34} Journalists Michael Barbaro and Tom Zeller, Jr. were able to take the anonymous searches of one user and use all of the information to discover her identity.\textsuperscript{35} Although AOL apologized and admitted that the release of the information was not authorized,\textsuperscript{36} it illustrates the ease with which someone with minimal research savvy and access to such information could identify each user and potentially use the information to commit identity theft or credit card fraud.

\textsuperscript{27}KRISTEN PURCELL, PEW RESEARCH CTR., SEARCH AND EMAIL STILL TOP OF THE LIST OF MOST POPULAR ONLINE ACTIVITIES: TWO ACTIVITIES NEARLY UNIVERSAL AMONG ADULT INTERNET USERS 2-3 (2011).

\textsuperscript{28}See, e.g., Ron A. Dolin, Search Query Privacy: The Problem of Anonymization, 2 HASTINGS SCI. & TECH. L.J. 137, 137 (2010).

\textsuperscript{29}In Search of Online Privacy, THE INDEP., Apr. 9, 2008, http://commens.org/sbMQS2 (asserting that Google, for example, retains this data for up to 18 months; and other popular search sites do so for a similar period).


\textsuperscript{31}Id. See also discussion, infra Part II.A.2.

\textsuperscript{32}Dolin, supra note 28, at 139.

\textsuperscript{33}See Michael Barbaro & Tom Zeller, Jr., A Face is Exposed for AOL Searcher No. 4417749, N.Y. TIMES (Aug. 9, 2006), http://commens.org/vFowka.
2. Behavioral Tracking and Advertising

Search engines are not the only way companies can track an individual's Internet use—most Web sites constantly collect data about their visitors. Anyone who has used a popular Web site like Netflix, Amazon, eBay, or Facebook can recall being required to enter personal information such as name, address, birthday, and email address to fully utilize the features of the site. While these practices seem appropriate given that sites need things like credit card billing information in order to fully serve their users, the public could be adversely affected if the information is not properly protected and falls into the wrong hands. For instance, a Carnegie Mellon University study found that 87% of the U.S. population could be identified by name solely by using their zip code, gender, and date of birth, all of which many Web sites contain.

Web sites may also collect data unbeknownst to web surfers through the use of tracking cookies. Tracking cookies are text files unknowingly downloaded onto a user's computer when he or she visits a specific Web site. These files log data, including the particular pages a user views on a Web site, how long he or she spends on each page, and what advertisements are clicked on. They also may store passwords, credit card information, or items a person may place in their shopping cart, which will be saved for when he or she returns to the Web site at a later time. Many sites use this cookie data to tailor content and product recommendations to the user on subsequent visits, all of which can make web browsing much more convenient and enjoyable.

If a user does not want a cookie to collect information, he or she can simply delete the cookie through the browser. Some web browsers give a user the

---

37 Hirsch, supra note 30, at 445-46.
41 HARRY NEWTON, NEWTON’S TELECOM DICTIONARY 317 (25th ed. 2009).
42 See id. See also FTC 2009 REPORT, supra note 40, at 2 n.3.
43 FTC 2009 REPORT, supra note 40, at 2 n.3.
44 Id.; NEWTON, supra note 41, at 317.
45 FTC 2009 REPORT, supra note 40, at 26 (recommendations include: tailored content, shopping cart services, website design and optimization, fraud detection, and security).
46 See, e.g., How to Delete Cookie Files in Internet Explorer, MICROSOFT.COM, http://commcns.org/uMKV7r (last visited Dec. 15, 2011); Firefox Help – Firefox and
option of rejecting a cookie before it has a chance to be downloaded. However, the biggest privacy concerns are with third party cookies, which are “placed on a user’s computer by a third-party, for example, a Web advertising company . . . through an agreement with the owner of the Website that the user is visiting.” After a third party cookie is installed on a user’s computer, it can follow a user to all the sites that have an agreement with the web advertising company.

Even with the ability to disable cookies, users may still be tracked by more advanced technologies, such as flash cookies. Flash cookies store data in a similar way to regular tracking cookies, but instead are downloaded into a computer by Web sites that use Adobe Flash player, rather than a browser. Deleting flash cookies requires a user to first be aware that the cookies are installed on their computer, and then follow instructions on Adobe’s Web site to remove them. If not deleted, flash cookies can be used to restore regular cookies, even if the regular cookies have been deleted.

Another advanced technology is web beacons, also known as web bugs or pixels. Rather than tracking users by embedding a text file on their computers, web beacons embed pieces of software code onto a Web site in order to track a user’s movements on the particular individual Web site. While profiles compiled by web beacons are supposed to be anonymous, companies have begun compiling information such as the types of movies an individual watches or the kind of news they read and selling such data to advertising companies.

The most alarming facet of Internet tracking is that even though it has become a common practice, some major Web sites are unaware that outside companies are placing tracking software on their Web sites. For instance, an


47 NEWTON, supra note 41, at 317.
48 Id. at 1118.
49 Id. at 317. See also discussion, infra Part II.B.
50 FTC 2010 REPORT, supra note 12, at 65-66.
51 Id. at 66 n.154.
52 Id.
53 Id.
56 Id.
57 Angwin, supra note 7.
58 Id.
investigation by the Wall Street Journal uncovered that a visit to Comcast's Web site installed 55 Flash cookies on a user's computer. While Comcast claimed it was unaware of the cookies, if one of the largest providers of cable services is unable to protect itself from Internet tracking, the average Internet user stands no chance.

B. Who Uses Internet Tracking?

As discussed, Web sites use data collected from Internet tracking in order to target specific advertisements to users and make web browsing more convenient and enjoyable. However, Web sites are not the only entities that use this data. Network advertisers are the "principal users of online personal data," and include Internet giants, such as, Google, Yahoo, and Microsoft, as well as lesser-known advertising companies, such as, Adify, BlueKai, and Undertone Networks. These companies enter into agreements wherein they pay individual Web sites for collected personal data and the right to display advertisements on the Web site.

By contracting with hundreds, or even thousands, of Web sites, network advertisers can track the web behavior of individual users across the Internet, enabling them to create a detailed profile of a user's habits and preferences. As a result, the next time the user visits one of the network Web sites, the network advertiser can use the space it purchased from the Web site to tailor pertinent advertisements towards the user. For example, if a male user purchases a pair of dress shoes from a specific company's Web site, he may be subject to advertisements for the same shoe company, or other men's clothing companies, on other sites he visits after the purchase. While the subsequent Web sites may have nothing to do with men's shoes or clothing, the network advertiser can target these advertisements to the user based on his previous activity.

Additionally, a secondary market for personal data culled from Web sites

59 Id.
60 Id. (according to Comcast, after being unaware of the occurrence, Comcast subsequently determined that it had used a piece of free software from a company called Cearspring Technologies Inc. to display a slideshow of celebrity photos on Comcast.net and that the Flash cookies were installed on Comcast's site by that slideshow).
61 See discussion, supra Part II.A.
62 Hirsch, supra note 30, at 447.
64 Hirsch, supra note 30, at 448.
65 Id. at 447-48.
66 Id.
has developed, enabling companies to buy data from Web sites and sell it to other entities. For example, eBay and Expedia sell personal data collected on their Web site to data brokers like BlueKai. Just moments after a user logs onto either eBay or Expedia, BlueKai auctions the user's information off on a "data exchange," selling as many as 50 million pieces of information each day. While BlueKai claims that all of this information is anonymous, an individual visiting BlueKai's Web site can find a variety of personal information, including age, household income, stores shopped at, types of brokerage accounts owned, and sports preferences. Most alarming to consumers, however, is that they have never heard of BlueKai and never consented to any of the information being collected, much less bought and sold. While consumers do have the option of opting out of being tracked, it is difficult to opt out of something they do not even know exists.

III. HISTORY OF THE FTC'S PRIVACY OVERSIGHT AND ITS DO NOT TRACK PROPOSAL

A. FTC Authority and Actions

The Federal Trade Commission Act of 1914 ("FTC Act") established an "independent and powerful antitrust enforcement agency" to prevent "unfair methods of competition . . . and unfair or deceptive acts affecting commerce." Created in response to the Supreme Court's dissolution of Standard Oil due to Sherman Antitrust Act violations, the Federal Trade Commission ("FTC") did not become involved in protecting consumer privacy until the enactment of the Fair Credit Reporting Act ("FCRA") in 1970. Prior to the enactment of FCRA, the credit reporting industry had been unregulated. By the late 1960s, U.S. credit bureaus had amassed files on over 110 million consumers, containing information such as Social Security

---

67 Angwin, supra note 7.
68 Id.
69 Id.
70 Id.
74 Crane, supra note 73, at 20.
numbers, mortgage and credit card accounts, and any outstanding balances, liens, and bankruptcy records.77 With privacy becoming a bigger concern as the industry grew, the Act’s purpose was to “balance the need for accessible credit data with consumers’ privacy concerns.”78 Namely, it set guidelines governing the collection and sharing of an individual’s credit information by credit bureaus and gave the FTC broad regulatory authority to achieve credit privacy goals.79

Since then, Congress has tasked the FTC with even greater regulatory oversight regarding consumer privacy. In 1999, Senators Phil Gramm, Jim Leach, and Thomas J. Bliley, Jr. authored the Gramm-Leach-Bliley (“GLB”) Act, repealing parts of the Glass-Steagall Act that prohibited banks from merging with financial institutions that participated in securities markets.80 To limit any negative privacy consequences of potential mergers, GLB requires financial institutions to provide annual notices about their privacy practices to customers; provide customers with the ability to opt out of having their information shared with third parties; and promote in house data security policies.81 The FTC is one of several federal agencies tasked with enforcing these requirements.82 However, the legislation has received criticism for failing to actually enhance consumer privacy protection—for instance, former FTC Chairman Timothy Muris noted that GLB simply created a “blizzard of barely comprehensible privacy notices.”83

B. The FTC’s Evolving Approach to Internet Privacy

Over the years, the FTC has developed two approaches to guide industry’s Internet data collection practices. In the 1990s, the FTC promulgated “fair information practice principles” that focused on giving consumers notice, choice, access, and security in regards to a company’s data collection

77 Id. at 3-4.
78 Id.
79 Id.
82 15 U.S.C. § 6805. (2006). The other agencies include the Board of Governors of the Federal Reserve System, the Office of the Comptroller of Currency, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, the National Credit Union Administration Board, the Securities Exchange Commission, and state insurance authorities. Id. §§ 6805, 6809(2).
83 Janger & Schwartz, supra note 80, at 1220; Munis, supra note 80.
practices. In the 2000s, as the Internet developed even more and became increasingly pervasive in everyday life, the Commission developed a "harm-based approach" that zeroed in on specific corporate data practices that harmed individuals. Armed with these tools, the FTC was able to pursue legal action against Internet companies that violated consumer privacy principles.

1. Fair Information Practice Principles

The FTC first addressed consumers' concerns over online privacy in the 1990s, just as online commerce began to take hold. The agency developed its own "Fair Information Practice Principles" ("FIPPs") in an attempt to allay concerns, focusing on four facets:

1. Businesses should provide notice of what information they collect from consumers;
2. Consumers should be given choice about how information collected from them may be used;
3. Consumers should have access to data collected about them; and
4. Businesses should take reasonable steps to ensure the security of the information they collect from consumers.

The Commission also identified enforcement as a critical component of any regulatory or self-regulatory program. Through this notice and choice approach, the FTC hoped to emphasize transparency and accountability in the way personally identifiable information was collected and disseminated. The Commission hoped that industry self-regulation would suffice; however, by 2000 only 32% of all privacy policies adequately met the four FIPPs. As a result, it recommended that Congress enact laws making FIPPs compliance mandatory for online businesses. While Congress never acted on this suggestion, the Commission was able to use its authority "to bring actions against companies that engaged in unfair or deceptive information practices . . . [that] involved deceptive . . . privacy notices about their collection and use of consumers' data."

---

84 FTC 2010 REPORT, supra note 12, at 6.
85 Id. at 9.
86 See infra note 99.
87 FTC 2010 REPORT, supra note 12, at 6.
89 FTC 2010 REPORT, supra note 12, at 6-7 (emphasis in original).
90 Id. at 9.
92 Id. at 36-38.
93 FTC 2010 REPORT, supra note 12, at 8.
94 Id. at 8-9. See, e.g., In re GeoCities, Inc., 127 F.T.C. 94 (1999) (consent order)
Despite its modest early success through lawsuits, the FTC realized that the notice-and-choice model was limited,\(^9\) noting that “[p]rivacy policies have become longer, more complex, and, in too many instances, incomprehensible.”\(^9\) Furthermore, these policies tended to limit liability rather than alert users about a site’s data privacy policies and rarely granted users the ability to control or opt out of data collection.\(^9\)

2. Harm-Based Approach

In the early 2000s, as offline and online data systems slowly began to blend together, the FTC moved to a harm-based approach that “targeted practices that caused or were likely to cause physical or economic harm, or ‘unwarranted intrusions in consumers’ daily lives.’”\(^9\) This new approach enabled the Commission to bring causes of action against many companies, including Microsoft and LexisNexis, for their failure to protect consumer information, as well as other suits for unwanted spam, spyware, and violations of legislation discussed above.\(^9\) Through these actions, the Commission was able to set precedents for protecting personal privacy, notify companies who handled personal information that they must develop effective policies to ensure personal privacy, and even obtain monetary rewards for consumers who’s privacy was violated by the companies.\(^10\)

Unfortunately, the harm-based approach is not without limitations. For example, the “harms” are narrowly focused only on “physical or economic injury” and “unwarranted intrusion[s] into consumers’ daily lives.”\(^10\) This limited definition completely ignores other harms that may concern consumers,
including reputational harm or the fear of being monitored and tracked.\textsuperscript{102} Furthermore, technological advances have enabled companies to collect and manage personal data at ever increasing rates while costs have significantly fallen.\textsuperscript{103}

3. **Specific FTC Efforts Regarding Online Privacy**

The rapid growth and evolution of the Internet and technology has presented regulators with a number of important privacy issues. One such problem is spyware.\textsuperscript{104} While Congress has not explicitly given the FTC regulatory authority over spyware, the agency has “broadened the range of practices that trigger privacy concerns to include software that collects and transmits information about users, their computers, or their use of the content.”\textsuperscript{105} As a result, the FTC has initiated actions against companies using illegal spyware by relying on its mandate to prevent “unfair or deceptive” trade practices.\textsuperscript{106} After investigating, the agency discovered that most of these cases centered around the issue of whether consumers had actually provided consent for a company to install spyware on their computer.\textsuperscript{107} Oftentimes, notice of the spyware installation was buried in end-user license agreements or other inconspicuous places, which the FTC found to be insufficient notice and, therefore, a deceptive practice.\textsuperscript{108}

The FTC also continues to tackle the problem of email spam. While Congress’ 2003 passage of the CAN SPAM Act empowered the FTC to bring criminal charges against individuals who send illegal mass emails, there have been issues with the implementation of the Act.\textsuperscript{109} For instance, CAN SPAM applies not only to illegitimate spammers, but also to subscription-only newsletters and corporate mailing lists.\textsuperscript{110} As a result, the Act has forced these

\textsuperscript{102} \textit{Id.}
\textsuperscript{103} \textit{Id.} at 21. See also discussion, supra Part II.
\textsuperscript{104} Spyware is “a type of software that is typically installed on a computer without the user’s knowledge and collects information about that user.” Kenneth A. Bamberger & Deirdre K. Mulligan, \textit{Privacy on the Books and on the Ground}, 63 \textit{STAN. L. REV.} 247, 290 (2011).
\textsuperscript{105} \textit{Id.} at 291.
\textsuperscript{106} \textit{Id.} at 290-91.
\textsuperscript{107} \textit{Id.} at 291.
entities to expend extra resources to comply with the law. Moreover, some have questioned whether the law is really necessary, given that most email providers now have inbox filters that remove spam. In fact, a 2009 study found that the Act had little to no effect on reducing unwanted spam and that compliance with CAN SPAM regulations had not increased.

The FTC has also attempted to safeguard the privacy of children on the Internet. Congress enacted the Children’s Online Privacy Protection Act (“COPPA”) in 1998, giving the FTC authority to regulate Web sites that target children. COPPA’s main objective was to require these Web sites to obtain parental consent before collecting and using personal information of children under thirteen. Additionally, the Act mandates that these Web sites notify parents as to what personal information they are collecting from children, allow parents to access any information collected about their children, refrain from collecting more information than necessary, and maintain reasonable procedures to keep the personally identifiable information confidential and secure. COPPA divides parental consent into two levels. Level one applies if a child’s information will be used only by the Web site collecting such information, and requires an email from a parent granting initial consent, followed by a “more secure” mechanism, such as a follow-up confirmation email. Alternatively, level two applies when information may be disclosed to a third party and requires the Web site obtain a parent’s written confirmation, verbal confirmation by phone, or confirmation by credit card payment.

Finally, the FTC has previously addressed the issue of online behavioral advertising. In 2009, the Commission released a report entitled “Self-Regulatory Principles For Online Behavioral Advertising” (“FTC 2009...
While the report is not binding on any entities, it sets guidelines for advertising where data is being shared with and used by a third party, like network advertising, rather than for any Web site collecting and using data itself. Moreover, it suggests Web sites collecting data to provide clear and concise notice that the user’s data is being collected and to offer users the opportunity to opt out of having their data collected. Finally, the report further suggests Web sites to provide reasonable security for the data and not retain it for longer than necessary.

However, if a Web site wants to use collected data in a substantially different way from the site’s original purpose, or if it wants to collect sensitive data for the purposes of behavioral advertising, it must obtain “affirmative express consent” from the user. Responding to the FTC 2009 Report, and hoping to stave off any similar legislation, the American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Directing Marketing Association, and Interactive Marketing Bureau joined forces to develop a self-regulatory framework that reflected the FTC report’s goals.

C. The FTC’s Proposed Privacy Framework

To address the mounting concerns regarding data collection and practices, the FTC held three public roundtables attended by “industry representatives, academics, technologists, consumer and privacy advocates, and government officials.” Incorporating ideas generated through these roundtables, the Commission generated a framework for consumer privacy that built upon both the notice and choice and harm based models, as well as previous FTC

---

120 See generally FTC 2009 REPORT, supra note 40.
121 Id. at 45-47.
122 Id. at 46.
123 Id. at 46-47.
124 The Commission refrained from explicitly defining “sensitive data” stating that it was “complex and may often depend upon context” and asked industry and consumer groups and other stakeholders to come up with a more specific standard. Id. at 44. However, the Commission did include “financial data, data about children, health information, precise geographic location information, and Social Security numbers” as examples of sensitive data. Id.
125 Id. at 47.
126 See generally AM. ASS’N OF ADVER. AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009) (setting out principles applying to educating consumers about online behavioral advertising, transparency and consumer control over data collection, data security, material changes in purpose, sensitive data, and accountability).
127 FTC 2010 REPORT, supra note 12, at 22.
regulations and policies.\textsuperscript{128} This framework identified three major guiding principles for all commercial entities that collect data on the Internet, calling on them to: (1) adopt “privacy by design” at every level of their operations; (2) simplify the way consumers are notified of their choices; and (3) be more transparent regarding their data practices.\textsuperscript{129} The Commission noted that the framework would apply to “commercial entities that collect consumer data in both offline and online contexts” who collect not just personally identifiable information (“PII”), but also “data that can be reasonably linked to a specific consumer, computer, or other device.”\textsuperscript{130}

1. \textit{Privacy by Design}

Under this principle, originally advocated by Dr. Ann Cavoukian, of the Ontario, Canada Information and Privacy Commissioner,\textsuperscript{131} a company that promotes consumer privacy at every level of their business and makes privacy an everyday practice.\textsuperscript{132} The FTC identified four protections for which companies must account.\textsuperscript{133} First, companies must provide reasonable security for any collected data, with the level of security directly proportional to the sensitivity of the data.\textsuperscript{134} For example, a Social Security number demands a higher level of security than a person’s favorite color.\textsuperscript{135} Second, companies must only collect data necessary for a specific purpose.\textsuperscript{136} Third, companies should retain data only as long as necessary and dispose of it once it is no longer needed.\textsuperscript{137} Finally, companies must implement procedures to ensure accuracy of the data they are collecting.\textsuperscript{138} The framework suggests that companies employ personnel whose job is to promote these privacy goals and train employees on privacy.\textsuperscript{139}

2. \textit{Simplifying Consumer Choice}

The FTC pointed out that even though most Web sites have privacy policies, these policies have become so drawn out and complex that most users are

\textsuperscript{128} \textit{Id.} at 39.
\textsuperscript{129} \textit{Id.} at 39-42.
\textsuperscript{130} \textit{Id.} at 42-43.
\textsuperscript{131} \textit{ANN CAUVIKIAN, INFO. & PRIVACY COMM’R OF ONT., PRIVACY BY DESIGN} 1.
\textsuperscript{132} \textit{FTC 2010 REPORT, supra} note 12, at 44.
\textsuperscript{133} \textit{Id.} at 44-48.
\textsuperscript{134} \textit{Id.} at 44-45.
\textsuperscript{135} \textit{Id.} at 45.
\textsuperscript{136} \textit{Id.} at 45-46.
\textsuperscript{137} \textit{Id.} at 46-47.
\textsuperscript{138} \textit{FTC 2010 REPORT, supra} note 12, at 48.
\textsuperscript{139} \textit{Id.} at 49.
unable to understand exactly what the company is doing with their personal
information, if they read them at all.\textsuperscript{140} As a result, the agency proposed a more
"streamlined choice model," with the purpose of preventing consumer
confusion.\textsuperscript{141} However, the new model included a number of "commonly
accepted practices" ("CAPs")\textsuperscript{142} for which companies did not need to seek
consent, including:

\textbf{Product and service fulfillment}: Situations where Web sites collect consumers' contact information in order to ship requested products or credit card information for payment. Also includes online tax calculators and financial analysis applications that collect financial information to run analysis for customers.

\textbf{Internal operations}: Instances where hotels and restaurants collect customer satisfaction surveys to improve customer service or when Web sites collect information about visits and click-through rates to improve site navigation.

\textbf{Fraud prevention}: Cases where offline retailers check drivers' licenses when consumers pay by check to prevent fraud or when online businesses employ fraud detection services to prevent fraudulent transactions. Also allows online businesses to scan web server logs to detect fraud and delete the logs when they are no longer necessary for this purpose.

\textbf{Legal compliance and public purpose}: Includes search engines, mobile applications, and pawn shops who share customer data with law enforcement agencies in response to subpoenas.

\textbf{First-party marketing}: Situations where online retailers recommend products and services based upon consumers' prior purchases on the website or offline retailers offer coupons to frequent purchasers of a specific good.\textsuperscript{143}

Since these types of data collection practices are obvious and often necessary, requiring consent would be more of a headache to consumers and businesses than any potential benefits accrued.\textsuperscript{144}

Consumers should be able "to make informed and meaningful choices" as to types of data collection that do not fall under CAPs, including companies selling information to data brokers, social media services with third party applications, and behavioral advertising.\textsuperscript{145} The FTC called for these choices to be described "clearly and concisely" through simple choice mechanisms offered in real time as the consumer is making the choice to provide data or not.\textsuperscript{146} It also noted that the invisibility of behavioral advertising required that consumers be provided with better tools to control such practices.\textsuperscript{147} While certain companies have already developed tools for consumers and web

\textsuperscript{140} See FTC 2009 REPORT, supra note 40, at 35.
\textsuperscript{141} FTC 2010 REPORT, supra note 12, at 52-53.
\textsuperscript{142} Id.
\textsuperscript{143} Id. at 53-54.
\textsuperscript{144} Id. at 54.
\textsuperscript{145} Id. at 57-58.
\textsuperscript{146} Id. at 58, 60-61. However, the Commission was noncommittal on whether the mechanism should be a choice to opt in or a choice to opt out. Id. at 60.
\textsuperscript{147} Id. at 63.
browsers now offer users the ability to set their own preferences regarding behavioral advertising, the Commission concluded that these efforts were insufficient. Instead, it called for the implementation of a uniform, browser-based mechanism called “Do Not Track,” which would signal to sites that a particular user does not want their data collected.

3. Increased Transparency for Data Practices

As discussed, consumers are frequently unaware that Web sites are collecting their personal data. Privacy policies do not adequately notify users of the data being collected and how such data is being used, often because the policies are lengthy and unintelligible to the average user. The Commission addressed this by setting out four specific goals, underscoring the need for companies to be more transparent about their data practices.

First, privacy notices must be “clearer, shorter, and more standardized” in order for consumers to better understand a Web site’s privacy practices, but must at a minimum include what data is being collected, why it is being collected and how it is being used. The FTC found success in the financial world by creating a model privacy notice for financial institutions to use in order to comply with the GLB’s requirement to send privacy notices to customers. Second, companies collecting data should allow consumers to access the information collected about them and to correct any incorrect information. At the time of the report, the Commission had sought comment from industry groups on the exact guidelines for consumer access.

Third, a company must get express consent from the consumers to use their data in a substantially different way than originally intended. This would apply especially to situations where social media sites like Facebook change default privacy settings, exposing private user data to third parties. Finally,


149 FTC 2010 REPORT, supra note 12, at 64-66.

150 Id. at 64-67.

151 See discussion, supra Part II.A.

152 FTC 2010 REPORT, supra note 12, at 69.

153 See generally id. at 69-79.

154 Id. at 70.

155 Id. at 71.

156 Id. at 72-74.

157 Id. at 75-76.

158 FTC 2010 REPORT, supra note 12, at 76.

159 Id. at 76-77.
the Commission stressed the need to increase consumer awareness of data collection, privacy issues, and tools available to users that enable them to control how they are tracked on the Internet. The FTC implored all stakeholders, not just companies and Web sites, to play a role in educating consumers about Internet tracking and privacy.\footnote{Id. at 78.}

D. Reaction and Criticism by Industry and Consumer Groups


\footnote{Simpson & Balber, supra note 164.}
that industry self-regulation would be insufficient.\footnote{Id.}

Explaining that trackers almost always win the “arms race between practical privacy tools and ubiquitous online tracking” because of the technology they utilize,\footnote{Peter Eckersley, What Does the “Track” in “Do Not Track” Mean?, ELECTRONIC FRONTIER FOUND. (Feb. 19, 2011), http://commcns.org/sMA4DK.} the Electronic Frontier Foundation (“EFF”) supported the fact that Do Not Track “creates a policy mechanism to augment the privacy enhancing technologies that we currently have.”\footnote{Id.} However, the organization also noted that many web browsers are already building Do Not Track mechanisms into their browsers and that legislation should be a last resort if companies do not voluntarily adopt the FTC’s proposed framework.\footnote{EFF Comment, supra note 164, at 13.} Furthermore, responding to industry criticism that the mechanism would cause great harm to the advertising industry, the EFF pushed the industry to innovate around any obstacles and develop new targeting methods that also protect consumer privacy.\footnote{Id. at 12.}

Likewise, the Center for Digital Democracy (“CDD”) and United States Public Interest Research Group (“U.S. PIRG”) conceded that Internet advertising provides several benefits to consumers,\footnote{CDD Comment, supra note 163, at 5.} but rejected claims that the health of the Internet would be threatened if the FTC enacted consumer privacy controls.\footnote{Id. at 6.} Furthermore, CDD and U.S. PIRG claimed that “[s]elf-regulation of online marketing to protect consumer privacy has been a failure from the start….\footnote{Id. at 12.} For example, until the FTC adopted COPPA and set guidelines for how Web sites targeted at children should approach self-regulation, these sites had taken little to no action to protect privacy.\footnote{Id. at 28.} According to CDD, therefore, until a statutory framework is in place, self-regulation will be wholly ineffective.\footnote{Id.} While they recognized the initiative of web browser companies in building some form of Do Not Track controls into their newest versions, CDD and U.S. PIRG reinforced the need for the FTC to be empowered to develop and enforce standards for a Do Not Track mechanism.\footnote{Id. at 37-38.}

The FTC’s minority criticized the concept of a Do Not Track mechanism, stating that such a mechanism would be too difficult to create.\footnote{Internet Privacy: The Views of the FTC, FCC and NTIA: Hearing Before H.} Specifically,
Commissioner William Kovacic called the proposal to implement a Do Not Track mechanism premature. Kovacic also wondered if there was really an effective way to enforce such a mechanism, with or without legislation. For instance, the proposed mechanism would “convey a consumer’s request not to be tracked, and would not actually prevent tracking.”

Commissioner J. Thomas Rosch also expressed serious reservations about the proposed framework, calling it “flawed” and unnecessary and pointing out that most consumers are not overly concerned with being tracked online. Rosch also disagreed that the notice model needed to be replaced, noting that it simply needed better enforcement requiring “notices to be clear, conspicuous and effective.” Furthermore, he cautioned that offering users opt-in or opt-out choices would actually “disincentivize [firms] from adopting acceptable privacy notices in the first place.” Rosch reserved his support for a Do Not Track mechanism only so far as it would be “technically feasible.”

Rosch also expressed wariness that Do Not Track could restrict competition, noting that while large firms like Google and Microsoft derive some revenue from behavioral advertising, they draw significantly more from search advertising. While losing revenue from behavioral advertising would have little effect on Google and Microsoft, other smaller firms could be crippled. Therefore, the Do Not Track mechanism could allow Google and Microsoft to use their power “to erect barriers to entry by which they can protect themselves from competition” and dominate the online advertising industry.

In its February 2011 initial public offering filing, Pandora, the free Internet radio Web site that tailors playlists to each specific listener, expressed concern that any Do Not Track mechanism would “significantly hinder [its] ability to


178 See FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT D-1 (2010) (Kovacic, Chairman, concurring) [hereinafter KOVACIC CONCURRING STATEMENT].

179 Id. at D-3.

180 Id.

181 See FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT E-1, E-4, n.6. (2010) (Rosch, Chairman, concurring) [hereinafter ROSch CONCURRING STATEMENT].

182 Id. at E-2, E-5.

183 Id. at E-3.

184 Id. at E-6.


186 Id.

187 Id.
collect and use data relating to listeners." The Interactive Advertising Bureau ("IAB"), an association representing over 470 advertising companies, proposed a self-regulatory approach allowing for "more flexibility to adapt to changing technologies while still enabling online advertising that helps" keep the majority of Internet content free. IAB argued that government regulation would quickly become obsolete "in the face of evolving technologies" and would stymie innovation. Self-regulation, on the other hand, has fostered competition and facilitated the development of opt-out mechanisms and privacy preference tools. Furthermore, a Do Not Track mechanism would propagate unwarranted consumer fear of legitimate and necessary data collection practices.

Moreover, Facebook maintained that industry self-regulation was the appropriate way to protect user privacy on the Internet. Like the IAB, Facebook emphasized the private sector's ability to react quickly to the evolving demands of the Internet and how the "user-driven" nature of the Internet allows users to be more involved in privacy solutions. Pointing specifically to the CAN SPAM Act, Facebook noted that the development of "sophisticated mail filters" by Internet service providers and email services "effectively addressed the problem of spam." As a result, the tedious process of passing legislation or agency rules would be much less effective than self-regulation aimed at adapting to privacy issues with new technology.

Industry groups also expressed concern about potential negative consequences of a Do Not Track mechanism. Blue Kai stressed that Internet advertisers would have to return to "interruptive" rather than "relevant" advertising, forcing Web sites to either charge users for content, show users advertisements before allowing them to view content, or both. This would be

---

189 IAB Comment, supra note 163, at 2.
191 IAB Comment, supra note 163, at 3.
192 Id. at 3.
193 Id. at 5.
195 Id. at 13.
196 Id. ("The ISPs' development of sophisticated mail filters that more effectively addressed the problem of spam.").
197 See id. at 14.
detrimental because, according to BlueKai, a majority of Internet users prefer free content with behavioral advertisements to pay for that content. Clickz, an online resource for Internet marketers, echoed these sentiments by stating that a Do Not Track mechanism would lead to "a higher volume of ads . . . less free, quality content . . . less relevant advertising . . . [and] intrusive ads." Clickz also warned that smaller Web sites might not have the budget to pay for the market research needed to sell advertisements so they can keep the Web sites running. Finally, ClickZ echoed sentiments for a self-regulatory regime by asserting that technology moves far too fast for government to properly regulate.

Likewise, the Direct Marketing Association ("DMA") underscored the benefits that data tracking and collection provided to both users and companies. For example, data tracking and personalized advertisements provide "valuable information to consumers and helps promote informed buying decisions." Moreover, targeted advertisements generate a much higher user response rate, lowering costs for Web site owners, which in turn benefits users in the form of lower prices. Lower advertising costs also allow smaller businesses easier entry into the marketplace and enhance competition. Agreeing that no new framework is necessary, the DMA explained that the notice and choice model and FIPPs have fostered technological innovation while remaining flexible to ensure users have sufficient control over private information. Finally, it stressed that "privacy by design" should not become a requirement because different types of entities have different necessities for data collection, retention, and use, making a "one size fits all" regulatory regime unsuitable.

Perhaps illustrating the point made by IAB, Facebook, Clickz, and many

---

199 Id.  
201 Id. at 5.  
202 Anna Maria Virzi, Do-Not-Track Deserves to Be Derailed, CLICKZ (Feb 18, 2011), http://commcns.org/uOS6NN.  
203 See DMA Comment, supra note 163, at 4-5.  
204 Id. at 5.  
205 Id.  
206 Id.  
207 Id. at 6, 9-10.  
208 Id. at 13-15.
others, Microsoft, Mozilla, and Apple have built mechanisms that allow users to control how their personal information is collected into their web browsers.\textsuperscript{209} Microsoft has even submitted its privacy framework to the World Wide Web Consortium ("W3C")\textsuperscript{210} for consideration as the industry standard.\textsuperscript{211} Furthermore, advertising companies are working in tandem with web browser companies to develop an effective and workable Do Not Track mechanism.\textsuperscript{212} As a result, while the FTC struggles with the question of whether a new Internet privacy framework with a Do Not Track mechanism should even be instituted, companies like Microsoft have already built in such a mechanism and are proposing new industry standards.\textsuperscript{213}

IV. PROPOSED LEGISLATION

A. Do Not Track Me Online Act of 2011: A Knee Jerk Reaction to Consumer Concerns

In early February 2011, Rep. Jackie Speier (D-CA) introduced the Do Not Track Me Online Act of 2011.\textsuperscript{214} The proposed Act mandates the FTC to

\textsuperscript{209} Wingfield & Angwin, supra note 148; Tsukayama, supra note 148; Wingfield, supra note 148. Google has so far refused to build such a mechanism into its browser citing lack of consensus for the definition of “tracking.” Ryan Singel, Google Holds Out Against ‘Do Not Track’ Flag, WIRED.COM (Apr. 15, 2011), http://commcns.org/ujhSiC. They have created a mechanism that allows users to opt out of being shown targeted advertisements, but does not give users the ability to completely opt out of being tracked. Greg Keizer, FTC Calls Out Google’s Chrome Over Do Not Track, COMPUTERWORLD (Apr. 20, 2011), http://commcns.org/vhpPOT.  


\textsuperscript{211} Robert Vamosi, Protect Your Online Privacy (Without Reading All the Fine Print), PCWORLD (Mar. 30, 2011), http://commcns.org/vnloc3.  


\textsuperscript{214} See Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011). Sen. John D. Rockefeller introduced a similar bill in May 2011. See Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011). Owing to the fact that both bills instruct the FTC to develop requirements for a Do Not Track mechanism, and Sen. Rockefeller’s bill is even less comprehensive than Rep. Speier’s bill, only the latter is discussed in this comment.
develop requirements for a Do Not Track mechanism,\(^{215}\) which would prohibit covered entities\(^{216}\) from collecting and storing a user’s personal information if the user opts out of being tracked.\(^{217}\) The bill also would require covered entities to inform users about the types of information it collects as well as how that information will be used.\(^{218}\) Furthermore, the bill allows, but does not require, the FTC to compel covered entities to provide a notice of the security policies and a means by which consumers can view the personal data that has been stored.\(^{219}\)

Along with new restrictions, the bill provides the FTC with authority to exclude any “commonly accepted commercial practices” from enforcement.\(^{220}\) Such practices may include things like customer service and support where collecting personal data is necessary, analyzing data to improve services and support, protecting intellectual property against security threats or other illegal activities, and preventing imminent personal injury.\(^{221}\)

However, aside from the mandate for a Do Not Track mechanism, the bill fails to address any of the other goals set out in the FTC 2010 Report. While the report focused heavily on “privacy by design,” simplifying user choice, and enhanced transparency,\(^{222}\) the only topic addressed by the bill is its provision requiring covered entities to inform users of data practices, a form of increased transparency.\(^{223}\) With Commissioners Kovacic and Rosch expressing so much concern over a Do Not Track mechanism and cautioning the public that the proposed privacy framework is still in the early stages of evaluation,\(^{224}\) it seems Rep. Speier may be jumping too far ahead of the FTC, especially since the feasibility of a Do Not Track mechanism is still very much in question.\(^{225}\) Even though web browsers are able to give users the option of not being tracked, there is no way for these browsers to actually prevent Web sites from

\(^{215}\) Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(a) (2011).

\(^{216}\) Id. § 2(2) (“The term ‘covered entity’ means ‘a person engaged in interstate commerce that collects or stores online data containing covered information. Such term does not include (A) the Federal Government or any instrumentality of the Federal Government, nor the government of any State or political subdivision of a State; or (B) any person that . . . (i) stores covered information from or about fewer than 15,000 individuals; (ii) collects covered information from or about 10,000 individuals during any 12-month period; (iii) does not collect or store sensitive information; and (iv) does not use covered information to study, monitor, or analyze the behavior of individuals as the person’s primary business.’.”).

\(^{217}\) Id. § 3(a), 3(b)(2).

\(^{218}\) Id. § 3(b)(1).

\(^{219}\) Id. § 3(c)(1).

\(^{220}\) Id. § 3(d).

\(^{221}\) Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(d) (2011).

\(^{222}\) See discussion, supra Part III.C.

\(^{223}\) H.R. 654 § 3 (b)(1).

\(^{224}\) See discussion, supra Part II.D.

\(^{225}\) ROSCH CONCURRING STATEMENT, supra note 181, at E-6.
tracking users.\textsuperscript{226} It is incumbent on both advertising networks and Web sites to honor a user’s preference in order for the mechanism to work effectively; unfortunately, advertisers have resisted to this task.\textsuperscript{227}

B. BEST PRACTICES Act: A More Comprehensive and Effective Framework for Internet Privacy

In early February 2011, Rep. Bobby Rush reintroduced the BEST PRACTICES Act ("Rush Act"),\textsuperscript{228} which he originally introduced near the end of 2010.\textsuperscript{229} Though the bill does not mandate a Do Not Track mechanism, it takes a more comprehensive approach to Internet privacy reform, addressing in part each of the three goals outlined in the FTC 2010 Report.\textsuperscript{230}

As noted, the FTC 2010 Report stressed simplifying consumer choices and increasing transparency in regards to data collection, but also embraced CAPs that were exempt from consent requirements.\textsuperscript{231} The BEST PRACTICES Act addresses most of these goals in Titles I and II.\textsuperscript{232} Covered entities\textsuperscript{233} would be required to notify users of the options they have for limiting data collection, as well as what type of data is being collected, the purpose for the collection, the manner in which the data would be used, and any third parties with which the data would be shared.\textsuperscript{234} Users must be notified of all of this information through “concise, meaningful, timely, prominent, and easy-to-understand . . .

\textsuperscript{226} Valentino-Devries, \textit{supra} note 212.

\textsuperscript{227} \textit{Id.}


\textsuperscript{231} See discussion, \textit{supra} Part III.C.2-3.

\textsuperscript{232} H.R. 611 §§ 101-106.

\textsuperscript{233} \textit{Id.} § 2(3) ("The term ‘covered entity’ means a person engaged in interstate commerce that collects or stores online data containing covered information. Such term does not include (A) the Federal Government or any instrumentality of the Federal Government, nor the government of any State or political subdivision of a State; or (B) any person that . . . (i) stores covered information from or about fewer than 15,000 individuals; (ii) collects covered information from or about 10,000 individuals during any 12-month period; (iii) does not collect or store sensitive information; and (iv) does not use covered information to study, monitor, or analyze the behavior of individuals as the person’s primary business.").

\textsuperscript{234} \textit{Id.} § 101.
notices before any data is collected and must be allowed, at any time, to opt-out permanently from having their data collected, while maintaining the ability to opt back in if they so choose.

Rep. Rush also included certain instances where consent is unnecessary, similar to CAPs. These include trade secret information, “operational purposes,” fraud detection, imminent danger, compliance with the law, and publicly available information. Once data has been collected, covered entities must ensure that users are given reasonable access to this data. In addition, as the FTC 2010 Privacy Report suggested, the covered entity must provide notice to the user and obtain express affirmative consent from the user if it wants to use the data in any way that is materially different from its original intent.

Title III of the Act sets out requirements for what resembles “privacy by design.” It would require covered entities to build safeguards into their systems to ensure proper security and protection of collected data. Such safeguards must account for “(1) the size and complexity of an entity; (2) the nature and scope of the activities of an entity; (3) the sensitivity of the information; (4) the current state of the art in . . . safeguards for protecting information; and (5) the cost of implementing such safeguards.” Furthermore, covered entities would be required to ensure that collected data is accurate for each individual user and conduct a risk assessment of its data practices, including disposing data once it is no longer necessary for its original intended purpose.

Rep. Rush also heeded calls from the industry, advancing a self-regulatory scheme that includes a safe harbor from private liability. Under the proposal,
businesses could submit a self-regulatory framework proposal known as a "Choice Program" to the FTC for review.247 Once approved, any covered entity may opt to participate in the approved Choice Program, exempting them from certain provisions of the bill.248 To be approved, the framework must include—among other things—mechanisms that prohibit a covered entity from providing collected data to a third party, ability for users to set preferences for how their data is collected, procedures for approving covered entities that want to opt into the proposed Choice Program, and penalties for noncompliance with the Choice Program.249 The Do Not Track framework Microsoft submitted to W3C for approval could potentially qualify as a Choice Program.250

Despite the consistency with the FTC 2010 Report, there is one alarming aspect of the BEST PRACTICES Act. Under Rep. Rush's proposal, covered entities would be exempt from obtaining consent for the collection and use of de-identified data.251 As noted, though de-identified data has been stripped of any supposed personally identifiable information, this information can be combined to ascertain the identity of an individual.252 However, the bill attempts to rectify this issue by including a provision that prohibits the reconstruction of data for this exact purpose.253

As discussed, Rep. Speier's bill mandates the FTC to come up with requirements for a Do Not Track mechanism, but ignores the macro goal of establishing a comprehensive, workable privacy framework for the Internet.254 While it does provide the agency with 18 months to institute a Do Not Track framework, it fails to include input on a privacy framework from industry groups, with whom the government must work with to develop a workable framework.255 With questions already looming as to the feasibility of a Do Not Track mechanism, the additional lack of a complementary privacy framework

247 Id. § 402(a).
248 Id. § 401.
249 Id. § 403.
251 H.R. 611 § 501(a).
252 Barbaro & Zeller, supra note 33.
255 Id. Compare with H.R. 611 §§ 401-404 (providing safe harbor provisions and the Self Regulatory Choice Program to industry participants in exchange for their cooperation).
would ensure that such a mechanism would fail. Simply telling firms what they cannot do is not enough to ensure that the entire Internet ecosystem properly protects user data. Firms need some type of uniform standard that will provide them with guidance on exactly what is required of them to ensure the security of user information.

Alternatively, Rep. Rush’s bill presents an extensive framework addressing all aspects of the FTC 2010 Report, while also allowing for a degree of industry self-regulation through the proposed Choice Program. The industry also has shown more eagerness to address the issue, as advertising companies have begun to work with Web browser developers to determine the effectiveness of a Do Not Track mechanism. Moreover, major industry groups have developed principles for third party behavioral advertising, which easily could be adapted to all behavioral advertising. Furthermore, the BEST PRACTICES Act encourages the government to work with industry groups and consumer advocates to develop the most effective framework for Internet privacy, regardless of whether it includes a Do Not Track mechanism. The input from industry and consumer advocates will be invaluable to the FTC and will enable it to consider all angles of data privacy and security. Unlike Rep. Speier’s bill, Rep. Rush’s bill will allow the FTC to develop a framework with uniform standards that will not only ensure the proper level of data privacy, but also provide industry with guidance on what exactly it must do to meet these standards. As a result, Rep. Rush’s bill more effectively ensures online consumer privacy, while allowing advertisers to generate the revenue necessary to keep Internet content free.

V. CONCLUSION

Behavioral advertising has brought great value to consumers and corporations alike, but these benefits have not come without serious concern. The rapid growth of the industry has pushed the issue of online privacy to the forefront of consumer consciousness. Copious amounts of personal data are constantly being bought and sold, usually with little consumer control or knowledge. While the government, industry, and consumer groups all have opinions on a workable solution for this problem, the precise parameters of this

---


257 Valentino-Devries, supra note 212.


solution remain the topic of intense debate.

Regardless, privacy issues, growing public concern, and the subsequent legislation that has been proposed make clear that something needs to be done to address the issue. While the FTC continues to mull over 450 different public comments submitted in response to the FTC 2010 Report, the agency’s proposed framework and Do Not Track mechanism may do more harm than good in the long run. For example, if adopted, Web sites may be forced to charge for content and services as they lose the ability to tailor their advertisements. Additionally, given that the necessity and feasibility of a Do Not Track mechanism remains in question, it may be premature for Congress to pass any legislation on the matter. However, should any legislation be passed, Rep. Rush’s bill provides a much more comprehensive and effective solution than any of the other proposals offered.

---

261 Rosch, supra note 14.
262 Id.