I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Pulling Back the Curtain: Online Consumer Tracking

LAURA J. BOWMAN*

I. INTRODUCTION

Think of every webpage you visited in the last year, every link you clicked on, and every term you typed into a Google search bar. Imagine if all of that information was compiled and identified with your name. Now imagine that the list of websites you visited and words you searched was available for others to view: your boss, your insurance provider, the HR representative who is about to interview you, your parents, your spouse, and your children. Would you want anyone and everyone to know where you have been online and what words you searched? Would these people draw inaccurate inferences from this information? Could it reveal facts you wished to keep private? Technologies currently allow such a list to be compiled without the Internet user's knowledge, and it is possible for the list to be identified with that unique user. Further, these practices take place without any government regulation in the United States. If the areas of online consumer data collection and use remain free of regulation, the widespread availability of this information could become reality.

The online advertising industry evolves constantly, creating new and innovative ways to reach consumers and market products. The industry's techniques change faster than you can say "pay per click."[1] Today, "advertisers no longer want to just buy ads. They want to buy

---

*Laura J. Bowman is a member of the Ohio State University Moritz College of Law class of 2012.

[1] *See* Julia Angwin, *The Web's New Goldmine: Your Secrets*, WALL ST. J., July 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

access to specific people."[2] Companies use controversial, secret, undetectable, and evasive techniques to follow consumers online in order to gather and sell information about them. When consumers traded in their typewriters for computers, did they trade in their privacy too? In 1999, Sun Microsystems CEO Scott McNealy told consumers, "You have zero privacy . . . [g]et over it."[3] Despite the advances of the digital age and the sacrifices people are willing to make for the convenience of the Internet, consumers should not be forced to concede to zero privacy. The right to privacy, or the "right to be let alone," which Supreme Court Justice Louis Brandeis conceived of in 1890, still exists.[4] But just how far the concept of privacy should extend in today's digital age remains unclear.[5]

Online tracking and consumer advertising offer some benefits to consumers and are a mainstay of the industry, but without regulation the consumer's information remains subject to exploitation. The unregulated collection and use of consumer information may result in discriminatory practices, security breaches, and damage to the concept of liberty at the very core of American society.[6] Consumers generally are unaware of what information is gathered about their online behavior and how that information is shared, sold, and used.[7] And most consumers mistakenly believe that their information is protected under websites' existing privacy policies.[8] The consumer

---

[2] Julia Angwin & Jennifer Valentino-Devries, *Race Is On to 'Fingerprint' Phones, PCs*, WALL ST. J., Nov. 30, 2010, http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html.

[3] Nicholas Carr, *Tracking Is an Assault on Liberty, With Real Dangers*, WALL ST. J., Aug. 6, 2010, http://online.wsj.com/article/SB10001424052748703748904575411682714389888.html.

[4] Olmstead v. United States, 277 U.S. 438, 478 (1928). *See also* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[5] *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 479 (2010) ("It takes longer for laws to evolve than for digital technology to advance. This is particularly true of laws that involve basic human values, such as privacy and free speech," and "clearer identification of norms and values" is necessary before privacy laws can be appropriately written.).

[6] Carr, *supra* note 3.

[7] *See infra* note 20 and accompanying text.

[8] Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 ISJLP 723, 724 (2008) ("When consumers see the term 'privacy policy,' they believe that their personal information will be protected in specific ways; in particular,

privacy problems surrounding online tracking are compounded by the challenges faced when attempting to regulate these practices.

This Note begins with an overview of online consumer tracking methods and Part II discusses the developments in the online advertising industry. Part III discusses the risks associated with the collection and use of online consumer information. Part IV examines the United States' current governance in this area. Part V describes the difficulties regulators will face imposing regulations on an industry that has developed with few restrictions, and details the European Union's struggles when regulating online tracking. Part V provides an overview of Google's approach to consumer privacy in online consumer tracking and advertising. This Note concludes that, while there is no readily apparent solution to the privacy issues raised by online consumer tracking, it is clear that any regulation must strike a delicate balance in order to effectively protect consumer privacy while still allowing flexibility for ongoing technological advancements.

II. THE SPIES BEHIND THE (COMPUTER) SCREEN

The tracking, collection, and sale of online consumer information takes place every millisecond of every day. The problem is that this data is being collected and sold without consumer knowledge and with few legal limits.[9] The question of how to regulate not only the collection of consumer information but also the way the information is used and stored is a dilemma facing governments worldwide.[10]

---

they assume that a website that advertises a privacy policy will not share their personal information.").

[9] *See infra* Part IV.

[10] *See, e.g.*, Emma Portier Davis, *Internet: Analysis Parsing Art. 29 Targeted Ad Opinion Favoring Cookies Opt-In Differ on Its Impact*, 9 PRIVACY & SEC. L. REP. (BNA), at 988 (July 5, 2010) (highlighting the debate over the interpretation of the European Union's e-Privacy Directive, particularly the provisions regarding consumer consent for cookies); Frederic Debusseré, *The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?*, 13 INT'L J.L. & INFO. TECH. 70, 73 (2005) (A "critical analysis is made of the new European rules for the use of cookies."); Lilian Edwards & Jordan Hatcher, *Consumer Privacy Law 2: Data Collection, Profiling and Targeting* (July 16, 2009), Research Paper No. 1435105, http://ssrn.com/abstract=1435105 (noting that tracking technologies are "currently perplexing privacy advocates, privacy commissioners and the European Commission alike, while users are still largely ignorant of their existence"); Meglena Kuneva, *Consumer Privacy and Online Market*, BEUC Multi-Stakeholder Forum (Nov. 12, 2009), http://ec.europa.eu/archives/commission_2004-2009/kuneva/speeches_en.htm; Meglena Kuneva, *EU Consumer Comm'r, A Blueprint for Consumer Policy in Europe: Making Markets Work with and for People*, Lisbon Council Event (Nov. 5, 2009), http://ec.europa.eu/archives/commission_2004-

Examining the methods for tracking consumers online and the ways that information is used and sold reveals the problems and dangers of allowing the industry to remain unregulated.

A. SPIED ON: ONLINE CONSUMER TRACKING

Like a good spy, online user tracking has developed and adapted; it works among us—right under our noses—but remains elusive and secret. In 1994, online user tracking became possible with the invention of "cookies." But at that time, online advertising was rare.[11] Even when online ads gained popularity in the late 1990s, "[a]dvertisers were buying ads based on proximity to content—shoe ads on fashion sites."[12] After the dot-com bust, power shifted from websites to the online advertisers themselves.[13] This allowed advertisers to pay for ads only when a user clicked on them. Due to this change, sites and ad networks searched for a way to "show ads to people most likely to click on them" in order to get paid.[14] Now, another change has taken place: rather than paying for an ad on a specific webpage, advertisers "are paying a premium to follow people around the Internet, wherever they go, with highly specific marketing messages."[15] This new strategy is facilitated by spying on consumers' online behavior. Spying on Internet users has become one of the

---

2009/kuneva/speeches_en.htm ("[T]echnology never ceases to amaze and today we are faced with the relatively new issue relating to the online collection of personal and behaviour data . . . . being done on an unprecedented scale on a massive scale and mostly without any user awareness at all."); Ariane Siegel et al., *Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union*, 65 BUS. LAW. 285, 285 (2009) (noting that the United States, the European Union, and Canada are all faced with common online privacy concerns but that "each jurisdiction has developed its own unique approach to dealing with privacy").

[11] Angwin, *supra* note 1.

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.* Changes to Google's business model "reflect a power realignment online." For years, the strongest companies on the Internet were the ones with the most visitor traffic. Today, the power resides with those that have the richest data and are the savviest about using it. Jessica E. Vascellaro, *Google Agonizes on Privacy As Advertising World Vaults Ahead*, WALL ST. J., Aug. 10, 2010, http://online.wsj.com/article/SB10001424052748703309704575413553851854026.html.

fastest-growing businesses on the Internet, and the process is a complicated one.[16]

The process of tracking, collecting, and selling online consumer information is both swift and silent—happening almost instantly and without the consumer's knowledge. How? Tracking technologies such as cookies gather personal details about the consumer and identify characteristics about her,[17] including her favorite movies, television shows, and browsing habits.[18] That information is "package[d] . . . into profiles about individuals" which are constantly updated as consumers move about the Web.[19] The profiles are then sold to companies seeking to attract specific types of customers.[20] Recently, exchanges similar to the stock market have appeared where these profiles are bought and sold.[21] Various technologies have been created and adapted to meet the demands of this new market.

B. SPY KIT: TOOLS FOR TRACKING

As the Internet advertising industry has evolved, consumer tracking technology has changed to fit the needs of the industry. Technology has grown more powerful and more ubiquitous. Currently, the nation's most popular fifty websites, "which account for about 40% of the Web pages viewed by Americans," each install an average of "64 pieces of tracking technology onto the computers of visitors, usually with no warning."[22] A dozen of these sites each installed more than 100 pieces of tracking technology, typically without consumer

---

[16] Angwin, *supra* note 1.

[17] *Id.* For example, the code may identify a consumer as "a 26-year-old female in Nashville, Tenn." *Id.* This identification is created in part by capturing what consumers type in any website—a product review, comment on a movie, or their interest in weight loss or cooking.

[18] *Id.* Some online marketers allow consumers to see what they know, or think they know, about him or her. *See also infra* note 124 and Part V.C.

[19] Angwin, *supra* note 1.

[20] *Id.* For example, one consumer's profile can be sold "wholesale," included with a group of movie lovers for "$1 per thousand," or "customized," as "26-year-old Southern fans of '50 First Dates'." *Id.* This information can also be segmented down to an individual person. *Id.* (quoting Eric Porres, Lotame Solutions Inc. Chief Marketing Officer).

[21] *Id.*

[22] *Id.*

knowledge.[23] Technologies used for tracking constantly change and develop. Those most commonly used currently include cookies, web beacons, flash cookies, history sniffing, and device fingerprinting.[24]

1. COOKIES AND WEB BEACONS

Cookies are the original online consumer tracking technology. A cookie is a small text file that stores information on a computer's hard drive. When a user goes to a website for the first time, the website assigns her a unique identification number. That number is stored in the cookie along with other information like the webpages she visits on that site, the items placed in her shopping cart, and any information she provides, such as her name and billing address. That cookie is then placed on the user's hard drive.[25] The cookie allows that original site to remember her even after she has left and visited other, unrelated webpages. In order to continue tracking consumers as they move from website to website, advertisers created the "third-party cookie."[26] Advertisers use third-party cookies to track users as they

---

[23] *Id.*

[24] U.S. courts have held that cookies, the simplest tracking device, are legal, but have not ruled on the legality of more complex trackers. *Id.*; *see also In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 497 (S.D.N.Y. 2001); Jonathan Bick, *New Net-Use Tracking Tactics Capture Privacy Claims*, 27 E-COMMERCE L. & STRATEGY 1, 2 (2011) (Plaintiffs allege that "DoubleClick's practice of placing cookies on the hard drives of Internet users who accessed DoubleClick-affiliated Web sites constituted violation of the Stored Communications Act ('SCA'), the Wiretap Statute, and the Computer Fraud and Abuse Act." The court held that DoubleClick's use of cookies fell into the consent exceptions of those statutes because "when Internet users agreed to the terms and conditions of the DoubleClick-affiliated site, they essentially were consenting to those sites using their information.").

[25] Christina Tsuei, *How Advertisers Track You*, WALL ST. J., July 30, 2010, http://online.wsj.com/video/how-advertisers-use-internet-cookies-to-track-you/92E525EB-9E4A-4399-817D-8C4E6EF68F93.html.

[26] *Id.* The creators of the cookie technology were concerned about privacy issues and designed cookies in a way that would not allow information to continue to be stored as users leave the original site and browse others. However, advertisers worked around these limitations and created the "third-party cookie." *Id.* Third-party cookies allow the advertisers to show a user an ad for the product she just viewed on amazon.com, while she is reading the news on an unrelated site. *Id.*

browse multiple, unrelated webpages and to "build lists of pages that are viewed from a specific computer."[27]

In addition to recording the websites a consumer visits and the information she inputs, advertisers can now track every move of her mouse using web beacons. Web beacons are a similar but newer technology also known as "Web bugs" and "pixels." Beacons are small pieces of software running on a webpage that track "what a user is doing on the page, including what is being typed or where the mouse is moving."[28] Web beacons are also used in third-party tracking. Similar to third-party cookies, as the user moves about the Internet and visits a site also "affiliated with the same tracking company," the Web beacon "take[s] note of where that user was before, and where he is now." This allows the tracking company to build a "robust profile" for each user.[29] But advertisers have innovated further, adapting technologies that actually evade users' attempts to avoid being tracked online.

2. FLASH COOKIES OR ZOMBIE COOKIES

Flash cookies are a newer technology which create new privacy and legal issues. Flash cookies were originally created to save users' Flash video preferences, such as volume settings.[30] Advertisers have adapted this technology to help track online consumers. Flash cookies evade traditional methods of removal—they are not actually deleted when an online consumer uses her browser options to remove cookies.[31] Since advertisers are actually "circumvent[ing] a user's attempt to avoid being tracked online," this technology raises significant privacy issues.[32] Lawsuits are currently pending regarding this questionable practice.[33]

---

[27] Angwin, *supra* note 1. Third-party cookies are widely used. More than half of the United States' top 50 websites "installed 23 or more 'third party' cookies." At the highest end of the spectrum, "Dictionary.com installed . . . 159 third-party cookies." *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Barry M. Benjamin & Stephen W. Feingold, *Flash Cookies: Marketing Tactic Raises Privacy Concerns*, 16 CYBERSPACE LAW 12, 12 (2011).

[32] Angwin, *supra* note 1; *see also* Benjamin & Feingold, *supra* note 31 ("The use of Flash cookies troubles many consumers because it contravenes the currently-understood consumer expectation around managing cookies on their computers. Indeed, the use of

3. HISTORY SNIFFING

A recent lawsuit highlights a different invasive method that advertisers use to track Internet users: "history sniffing."[34] Because browsers display a website link in a different color when the browser has visited a webpage before, a company can tell whether a user has visited a particular site before simply by running a code in the user's browser and it can then create a profile based on the sites that user has viewed without the user knowing. History sniffing can be used to gather "extensive information regarding the domains or even

---

Flash cookies, which are not necessarily deleted when a consumer deletes regular cookies from her browser, may well contradict brand advertiser privacy policies.").

[33] *See* Jennifer Valentino-Devries & Emily Steel, *'Cookies' Cause Bitter Backlash*, WALL ST. J., Sept. 19, 2010, http://online.wsj.com/article/SB10001424052748704416904575502261335698370.html. *See also* Eric C. Bosset et al., *Private Actions Challenging Online Data Collection Practices Are Increasing: Assessing the Legal Landscape*, 23 INTELL. PROP. & TECH. L.J. 3, 3 (2011) (Recent lawsuits "allege that certain online marketing firms and their publisher affiliates improperly used 'local shared objects,' also known as 'Flash cookies,' to, for similar advertising reasons, track user activity and back up HTTP cookies for the purpose of restoring them later (also referred to as browser cookie re-spawning).") (internal citations omitted); Jessica E. Vascellaro, *Suit to Snuff Out 'History Sniffing' Takes Aim at Tracking Web Users*, WALL ST. J., Dec. 6, 2010, http://online.wsj.com/article/SB10001424052748704493004576001622828777658.html ?mod=WSJ_Tech_LEFTTopNews. One such suit alleging that Quantcast Corp., Clearspring Technologies Inc. and several other websites "used online-tracking tools that essentially hacked into users' computers without their knowledge" recently ended in a settlement. Under the settlement agreement, Quantcast and Clearspring agreed not to use Flash Cookies "to store Web-browsing activity without adequate disclosure or except related to Adobe System Inc.'s Flash program" and "to pay $2.4 million, some of which will go toward one or more online-privacy nonprofit organizations." The settlement remains subject to court approval. *See In re* Clearspring Flash Cookie Litig., No. 2:10-cv-05948-GW-JCG (C.D. Cal. filed Dec. 3, 2010); *In re* Quantcast Flash Cookie Litig., No. 2:10-cv-05484-GW-JCG (C.D. Cal. filed Dec. 3, 2010).

[34] Vascellaro, *supra* note 33; *see also* Kashmir Hill, *History Sniffing: How YouPorn Checks What Other Porn Sites You've Visited and Ad Networks Test the Quality of Their Data*, FORBES (Nov. 30, 2010, 6:23 PM), http://blogs.forbes.com/kashmirhill/2010/11/30/history-sniffing-how-youporn-checks-what-other-porn-sites-youve-visited-and-ad-networks-test-the-quality-of-their-data; Kashmir Hill, *Class Action Lawsuit Filed Over YouPorn History Sniffing*, FORBES (Dec. 6, 2010, 7:04 AM), http://blogs.forbes.com/kashmirhill/2010/12/06/class-action-lawsuit-filed-over-youporn-history-sniffing. ("The suit accuses YouPorn and the other sites of 'impermissibly accessing [users'] browsing history' and seeks class-action status. The lawsuit alleges that the porn websites broke California computer and consumer protection laws, as well as 'violat[ed] Plaintiffs' privacy interests.'"); *see also* Complaint at ¶¶ 15, 28, Pitner v. Midstream Media Int'l, N.V., (C.D. Cal. filed Dec. 6, 2010) (No. 8:10-cv-01850).

subdomains" a consumer visits, and because the code is delivered via ads or other items on a site, the site's host may not know that the history sniffing is taking place.[35] Federal Trade Commission (FTC) director David Vladeck noted with concern that "history sniffing 'deliberately bypassed' the most widely known method consumers use to prevent online tracking: deleting their cookies."[36] The FTC requested that browser vendors implement fixes to protect consumers from history sniffing. While some vendors have implemented these changes, the majority of Web users remain vulnerable and soon "more-sophisticated types of sniffing" may be developed, making current browser protections obsolete.[37]

4. DEVICE FINGERPRINTING

Yet another "new and controversial" tracking technique in the online advertising industry is device fingerprinting.[38] Every time a consumer goes online, his computer broadcasts hundreds of unique details as an identifier for the other computers it connects with. Each computer possesses a "different clock setting, different fonts, different software" and other specific characteristics that identify it.[39] Companies use this data to individually identify a computer and then track and build a profile of its user.[40]

Fingerprinting began as a way to stop the copying of computer software and prevent credit card fraud.[41] But it has become a powerful new tool for tracking companies. Not only is fingerprinting difficult to block, even "sophisticated Web surfers" cannot tell if their devices are

---

[35] Vascellaro, *supra* note 33.

[36] *Id.*

[37] *Id.*

[38] Jennifer Valentino-DeVries, *'Evercookies' and 'Fingerprinting': Are Anti-Fraud Tools Good for Ads?*, WALL ST. J. (Dec. 1, 2010, 10:49 AM), http://blogs.wsj.com/digits/2010/12/01/evercookies-and-fingerprinting-finding-fraudsters-tracking-consumers.

[39] Angwin & Valentino-Devries, *supra* note 2.

[40] *Id.* (noting that the same method can be used to identify and track cell phones and other devices).

[41] *Id.*

being fingerprinted.[42] Even if a user is aware of the fingerprinting, unlike cookies, there is no way for users to delete the fingerprints that have been collected.[43] This gives advertisers a significant advantage and companies utilizing fingerprinting expect to "completely replace the use of cookies."[44] Consumers may be surprised that they cannot avoid being tracked online without permission, but there is no regulation restricting these practices.

III. NOWHERE TO HIDE

There is currently no uniform federal regulatory system governing the collection and use of online consumer information. The risks associated with the unregulated collection and use of consumer information range from breaches and misuse of personal information to the crumbling of the freedoms which are the foundation of American society. It remains unclear which entity should regulate—Congress, the FTC, the Department of Commerce (DOC), or a White House commission—and what form regulations should take in order to effectively protect consumer privacy while still allowing flexibility for ongoing technological advancements. Thus far, regulation efforts have "resulted in a combination of legislation and promotion of industry self-regulation."[45] The federal government's "piecemeal approach" to protecting online privacy has been deemed inadequate for years by scholars and privacy advocates.[46] Regulation-free

---

[42] *Id.*

[43] *Id.* While most fraud-prevention companies keep fraud data and advertising data separate, some plan to combine the two, making it possible to identify the tracked consumer and giving rise to privacy issues. Companies also plan to link the profiles of devices that appear to be used by the same consumer and may even seek to match people's online data with offline information "such as property records, motor-vehicle registrations, income estimates and other details" which raises additional privacy concerns. *Id.*

[44] *Id.* ("Tracking companies are now embracing fingerprinting partly because it is much tougher to block than other common tools used to monitor people online such as browser 'cookies.'"). One company examined 70 million website visits and found that it could create a fingerprint for 89% of those visits. *Id.*

[45] Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 803 (2003).

[46] *Id.*; *see also* Alan F. Blakley et al., *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, DUKE L. & TECH. REV. 25, 25 (2005) ("Existing law does not address spyware adequately because authorization language, buried in 'click-through' boilerplate, renders much of current law useless. Congress must act to make spyware companies disclose their intentions with conspicuous and clearly-stated warnings.");

consumer tracking presents a serious threat to privacy.[47] Moreover, many online consumers are unaware of the collection and use of their online data. Finally, new technologies mean that anonymization—identification by a number rather than a person's name—can no longer be relied upon to shield the consumer's data from identification.

A. AN INVISIBLE ASSAULT ON PRIVACY

The fact that the majority of user data is collected without the user's knowledge raises significant privacy issues.[48] When consumers are kept unaware, "even the legal use of private information may be surprising and unnerving."[49]

If collected information falls into the wrong hands, "this information could facilitate identity theft, credit card fraud, cyber-stalking, damaged credit, and more."[50] Additional concerns surround

---

Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEG. COMMENT. 393, 395 (2002) ("The Internet poses a new set of challenges to privacy . . . . [b]ut the legal system has not sufficiently evolved and . . . . [t]he current policy of self-regulation whereby Internet users and operators are setting the rules and regulations has proven to be ineffective."); Amy S. Weinberg, *These Cookies Won't Crumble—Yet: The Corporate Monitoring of Consumer Internet Activity, In Re Doubleclick Inc. Privacy Litigation*, 21 TEMP. ENVTL. L. & TECH. J. 33, 33–34 (2002) (Congress is "considering the passage of new laws to cope with [online consumer tracking] issues. At this time, however, the practices of DoubleClick, Inc., for the purposes of research and enhancement of Internet usage, while seemingly improper, have been deemed to not be in violation of federal law.").

[47] David Bender, *Targeted Advertising Arrives on the Government's Radar*, N.Y. L.J. (April 7, 2009), http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202429695777. (Sir Tim Berners-Lee, considered the founder of the World Wide Web highlights some necessary considerations: "People use the Internet to search for information when they're concerned about their sexuality, when they're looking for information about diseases or when they're thinking about politics" and because of the private nature of information such as this, "it's vital that they are not being snooped on.").

[48] Brian Stallworth, Note, *Future Imperfect: Googling for Principles in Online Behavioral Advertising*, 62 FED. COMM. L.J. 465, 479 (2010) (noting, "Chief among the privacy concerns raised by online profiling [are] its nearly invisible nature and the broad scope of data collected about individual consumers").

[49] *Id.* at 473. ("Although millions of Americans appear willing to sacrifice a significant measure of their private information to gain access to Google's ever-increasing armament of products and services, these people may not fully appreciate the risks they are taking.").

[50] *Id.*

the breadth of the data that is collected and the risk that "[e]xcess customization of the Web experience may stratify society."[51] For example, if a user's profile suggests that he is "poor or from a minority group . . . the news, entertainment and commentary [he] sees on the Web might differ from others', preventing [his] participation in the 'national' conversation and culture that traditional media may produce."[52]

At the most basic level, the continuous, concealed collection of personal information online threatens "[t]he very idea of privacy."[53] Consumers value both personalization and privacy, and generally understand that they cannot have more of one without sacrificing some of the other. In order to have products and promotions tailored to a consumer's personal situation and tastes, he must divulge information about himself to corporations, governments, or other outsiders. While this tension has long been present in consumers' lives, covert online tracking eliminates consumers' ability to control the tradeoffs for themselves.[54] It remains unclear just how to empower consumers in a way that allows them to make decisions regarding their online privacy.

B. TOUGH COOKIES

There are numerous obstacles to consumer choice and lawmaker regulations in the area of online tracking. While some ad networks do

---

[51] Jim Harper, *It's Modern Trade: Web Users Get as Much as They Give*, WALL ST. J., Aug. 7, 2010, http://online.wsj.com/article/SB10001424052748703748904575411530096840958.html.

[52] *Id.*; *see also*, Jonathan Zittrain, *Let Consumers See What's Happening*, N.Y. TIMES, Dec. 2, 2010, http://www.nytimes.com/roomfordebate/2010/12/02/a-do-not-call-registry-for-the-web/let-consumers-see-whats-happening ("The real nightmare scenarios [of online tracking] are not better placed dog food ads. They have to do with varying price or service depending on undisclosed and long-collected behavior cues." For example, if a consumer's "life insurance rates were based not just on facts like a medical checkup, but unexplained variances in what Web sites you elected to visit.").

[53] Carr, *supra* note 3. *See also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 484 (2006) ("Privacy is the relief from a range of kinds of social friction. It enables people to engage in worthwhile activities in ways that they would otherwise find difficult or impossible."); Warren & Brandeis, *supra* note 4, at 198. ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.").

[54] Carr, *supra* note 3.

permit the savvy consumer to opt out of cookies and thus tracking via cookies, often "the opt-out must be renewed each time the user clears cookies from the browser."[55] Further, the technology used to enforce consumers' privacy preferences, such as cookie opt-outs are "ineffective in many instances" and "allow[] cookies to be downloaded to users regardless of their privacy settings."[56] In addition, tracking software operates on many websites without the website's knowledge. A recent study reports, "nearly a third of the tracking tools on fifty popular U.S. websites were installed by companies that gained access to the site without the [web site] publisher's permission."[57] If a company is not aware of tracking software, it cannot notify its users or provide them with options for protection. Furthermore, tracking technologies change rapidly. The industry has already passed through several waves of changing strategies and technologies.[58] Just as regulators have begun to focus on methods for regulating cookies, tracking companies are moving on to different techniques.[59] Changes in technology also mean changes to the data itself, leaving data that was previously "anonymous" now more easily identifiable.

C. THE CRUMBLING SHIELD OF ANONYMITY

For years advertisers said that the anonymity of online consumer data would shield the consumer from an invasion of privacy. But advances in technology can now leave a consumer and her identity exposed. Generally, the gathered information remains anonymous—a consumer is identified by a number assigned to the computer rather than the individual's name.[60] Proponents of tracking point to this

---

[55] Bender, *supra* note 47, at 5.

[56] *Internet: Cookie-Blocking Protocols on Many Sites Do Not Work, Mislead Users, Report Says*, 9 PRIVACY AND SEC. L. REP. (BNA), at 1329 (Sept. 27, 2010).

[57] Jessica E. Vascellaro, *Websites Rein in Tracking Tools*, WALL ST. J., Nov. 9, 2010, http://online.wsj.com/article/SB10001424052748703957804575602730678670278.html.

[58] *See supra* Part II.B.

[59] Angwin & Valentino-Devries, *supra* note 2 ("'I think cookies are a joke,' [David Norris, CEO of tracking company BlueCava Inc.,] says. 'The system is archaic and was invented by accident. We've outgrown it, and it's time for the next thing.'").

[60] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., Oct. 25, 2010, http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

"layer of anonymity" as "a reason online tracking shouldn't be considered intrusive."[61]

However, not every tracking company gathers only anonymous data. One online tracking company, RapLeaf, gathers information from a variety of sources, including "voter-registration files, shopping histories, social-networking activities and real estate;" RapLeaf's databases also include consumers' "real names and email addresses."[62] Currently, the company's database contains one billion email addresses.[63] RapLeaf claims to honor users' requests for removal from its system and has stated that it removes personally identifiable data from profiles prior to selling information for online advertising. But RapLeaf has "inadvertently" transmitted details that can identify a user, like a unique Facebook identification number, which links to a user's name, and a similar MySpace ID number that can be linked to an individual's name. RapLeaf states that this practice was stopped after it was told that this was occurring.[64] Still, the collection, storage, and use of consumer information that includes the consumer's name and email address raises significant privacy issues. The company's own lack of awareness of the use of its collected information highlights the need for regulations that will force companies to examine and enforce stringent policies for use of consumer data.

With the vast information that is collected nearly instantaneously as a consumer surfs the Web, she is often just "one more piece of information" short of being identified.[65] When AOL publicized three months' worth of the search terms used by 657,000 of its users, in anonymized form, the true sensitivity of this information became evident; despite the anonymization, the *New York Times* quickly identified "searcher No. 4417749 as an over-60 widow in Lilburn, Georgia, USA."[66] Similarly, in 2006, DVD rental company Netflix

---

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

[66] Edwards & Hatcher, *supra* note 10.

released "anonymous" data from 480,000 of its customers which included "100 million movie ratings, along with the date of the rating, a unique ID number for the subscriber, and the movie info" for a contest challenging participants to create a "recommendation algorithm that could predict 10 percent better than Netflix how those same subscribers rated other movies."[67] Only a few weeks after the contest began, two contestants "identified several Netflix users by comparing their 'anonymous' reviews in the Netflix data to ones posted on the Internet Movie Database website."[68] This revealed personal information such as political leanings and sexual orientation.[69]

A tracking company can access and analyze thousands of pieces of information about a consumer, including the individual's ZIP code and demographic group, in less than one second.[70] With this information, it is likely that only one more piece of information, such as a person's age or birth date, would allow de-anonymization.[71] While the cost of such de-anonymization for all entries in a company's database may exceed any benefits at this point in time, the possibility is real. Anonymity of data is neither guaranteed nor a foolproof substitute for regulation.[72] Regulation cannot rely on anonymization to protect individuals' privacy.[73]

---

[67] Ryan Singel, *Netflix Spilled Your Brokeback Mountain Secret*, Lawsuit Claims, WIRED MAGAZINE (December 17, 2009, 4:29 PM), http://www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit. One of the identified subscribers filed *Doe v. Netflix*, alleging Netflix violated fair-trade laws and federal privacy law. *See* Complaint, Doe v. Netflix, Inc., (N.D. Cal filed Dec. 17 2009) (No. C09-05903).

[68] *Id.*

[69] *Id.*

[70] Steel & Angwin, *supra* note 65.

[71] *Id.* (The information collected about one individual included income level, education, and town. This "narrow[ed] him down to one of just 64 or so people world-wide." And with "one more piece of information about him, such as his age" the specific individual could likely be identified.).

[72] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1743 (2009) (Computer scientists can now "reidentify" or "deanonymize" individuals from anonymized data with "astonishing ease," meaning that anonymization can "no longer be considered to provide meaningful guarantees of privacy.").

[73] *See id.* (Regulations such as the EU Data Protection Directive and the United States' HIPAA rely on anonymization as a privacy protection. Ohm urges the reevaluation of these

The anonymity of consumer data has recently been easily and unknowingly compromised by some of the biggest players in the Internet industry. Affiliates of both MySpace and Facebook have collected and shared tracking information, including a unique profile number associated with the user, despite policies prohibiting such practices.

1. MYSPACE

As with many websites, when a MySpace user clicks on an online ad, "pieces of data are transmitted, including the web address of the page where the user saw the ad."[74] However, on MySpace, this web address has included a user's unique ID number, giving its holder the ability to access that specific user's profile page. While some MySpace profiles use a "display name" rather than a person's actual name, the user ID provides access to all information that a person has made public on their profile.[75] The information was shared by applications or "apps" on the social-networking site. These apps let users play games and share information.[76] Unfortunately, the apps themselves were sharing information, despite the fact that MySpace policy prohibits this practice. This demonstrates how "fundamental Web technologies can jeopardize user privacy" and that a website's policies and terms may not go far enough to protect consumer information.[77]

2. FACEBOOK

Facebook uses tracking to learn about its 800 million users, but has had to change its practice of transmitting unique user ID numbers in addition to the information properly transmitted when a user clicks on an ad. A great deal of user activity on Facebook occurs using apps.

---

and "any law or regulation that draws distinctions based solely on whether particular data types can be linked to identity" as well as cautioning against the drafting of new laws or regulations based on this distinction.).

[74] Geoffrey A. Fowler & Emily Steel, *MySpace, Apps Leak User Data*, WALL ST. J., Oct. 23, 2010, http://online.wsj.com/article/SB10001424052702303738504575568460409331560.html.

[75] *Id.*

[76] *Id.*

[77] *Id.*

In 2011, it was discovered that for an undetermined amount of time, Facebook apps sent user information to advertising and data firms but included the user's Facebook ID number with that information. Several of the applications transmit personal information about the user's friends to outside companies. Even if a Facebook user has her profile set to "private," a search of the Facebook ID will reveal the user's name. Like MySpace, Facebook's policies "prohibit app makers from transferring data about users to outside advertising and data companies, even if a user agrees."[78] Clearly, merely having the policy is not enough to protect consumer privacy. Enforcing this policy on Facebook's 550,000 apps seems to have been a challenge and consumer privacy has suffered as a result.[79]

But even if the data is anonymous, the government's current privacy guidelines simply do not "adequately address growing societal concerns regarding the use and protection of information."[80] It is true that the regulation-free environment has allowed innovative new technologies to develop, many of which benefit both consumers and companies. But the lack of regulation in this area has resulted in a "trial-and-error" approach and has allowed companies to push the limits of privacy.[81] This lack of comprehensive regulation "creates uncertainty for businesses and consumers alike," and "will result in a

---

[78] Emily Steel & Geoffrey A. Fowler, *Facebook in Online Privacy Breach*, WALL ST. J., Oct. 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

[79] *Id.*

[80] Andrew B. Serwin, *Consumer Privacy: Privacy 3.0—A Reexamination of the Principle of Proportionality*, 9 PRIVACY & SEC. L. REP. (BNA), at 1230 (Aug. 23, 2010; *see also* Vascellaro, *supra* note 15.

[81] *See, e.g.*, Subrahmanyam KVJ, *Google Buzz's Privacy Breach is a Sign of things to Come*, VENTUREBEAT (FEB. 14, 2010), http://venturebeat.com/2010/02/14/google-buzzs-privacy-breach-is-sign-of-things-to-come/. Google pushed the privacy envelope in early 2010 with its social networking program, Google Buzz. Almost immediately, privacy concerns bombarded the Internet giant, which was forced to implement changes to the program and publicly apologize. A class action lawsuit alleged "Google automatically enrolled Gmail users in Buzz, and that Buzz publicly exposed data, including users' most frequent Gmail contacts, without enough user consent." Complaint, Hibnick v. Google Inc., (N.D. Cal. Feb. 17, 2010) (No. CV-10-672). In June of 2011, the class action settlement was approved, requiring Google to pay $8.5 million to various organizations and entities. *In re* Google Buzz User Privacy Litigation, Case No. 5:10-CV-00672-JW (N.D. Cal.) (Sept. 03, 2010).

continuation of the patchwork, and at times inconsistent" regulatory approach, which may not provide adequate protection to consumers.[82]

IV. CURRENT GOVERNANCE: RECOMMENDATIONS WITHOUT REQUIREMENTS

In the United States, the current governance of online consumer tracking consists of self-regulatory principles and a self-regulatory framework of best practices recommendations. While the FTC does not enforce these principles and framework because they are not mandatory, the FTC can bring an action against a company whose actions do not conform to its stated privacy policies, including any of the self-regulatory principles the company claims to follow. Congress has proposed legislation governing online consumer tracking on several occasions, but none has become law.

A. THE FTC'S RECOMMENDATIONS

In the area of online privacy, the FTC has "investigated fairness violations, brought law enforcement actions, required some Web sites to post privacy policies, and overseen an on-going dialog with industry and consumer groups."[83] But "concern for stifling the freedom and prosperity of online commerce" has hindered the FTC's ability to establish "enforceable regulatory privacy standards."[84] Thus far, the FTC has approached online behavioral advertising and tracking with only recommendations, not regulatory requirements.

1. THE FTC'S SELF-REGULATORY PRINCIPLES OF 2009

Following a 2007 "Town Hall" in which numerous industry leaders and interested parties discussed the benefits and concerns of online behavioral advertising, the FTC released a staff report with "Self-

---

[82] Serwin, *supra* note 80.

[83] Stallworth, *supra* note 48, at 468; *see generally*, Susan E. Gindin, Nobody *Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1 (2009) (discussing and analyzing the FTC's action against Sears Holding Management Corp. and its online privacy implications).

[84] Stallworth, *supra* note 48, at 468.

Regulatory Principles for Online Behavioral Advertising."[85] These principles included four "governing concepts." First, companies should inform consumers that they gather information for behavioral advertising and allow the consumer to choose whether or not to allow that practice. Second, companies should take reasonable measures to protect consumer data and should not retain the information longer than necessary. Third, if a company decides to use consumer data in a way that is "materially different" from its stated purpose when it collected the data, it should do so only after obtaining express permission from the consumer. Fourth, companies should obtain permission before using sensitive data for behavioral advertising.[86]

The self-regulatory principles were embraced by the industry,[87] but consumer advocate groups urged that the non-mandatory principles do not provide adequate consumer protections.[88] The nation's most prominent media and marketing associations created the Self-Regulatory Program for Online Behavioral Advertising (Industry Program). This Industry Program is based on the FTC's Self-Regulatory Principles and "gives consumers a better understanding of and greater control over ads that are customized based on their online behavior."[89]

---

[85] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING TRACKING, TARGETING, & TECHNOLOGY 1–2 (2009) [hereinafter FTC STAFF REPORT 2009], *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[86] *Id.* at 11–12. Sensitive data includes "data about children, health, or finances." *Id.*

[87] *See* AM. ASSOC. OF ADVER. AGENCIES ET AL., SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf (These Industry Principles "correspond with tenets proposed by the Federal Trade Commission in February 2009, and also address public education and industry accountability issues raised by the [FTC].").

[88] *See, e.g.*, Alexei Alexis, *Legislation: Business Lobbyists Press for Self-Regulation; Boucher Privacy Proposal Seen as Disruptive*, 9 PRIVACY & SEC. L. REP. NO. 23 (BNA), at 844–45 (June 7, 2010) ("Consumer advocates . . . remain dissatisfied with industry self-regulation and are urging congressional action. [In September 2009,] a coalition of advocacy groups called on Congress to impose tough privacy standards on online companies, including a 24-hour limit on the use of any personal data obtained without the consumer's prior consent and an absolute ban on the collection of sensitive information.").

[89] THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/home (last visited Sept. 23, 2011).

The Industry Program "requires participating firms to display an 'advertising option icon' within or near online ads or on web pages where data is collected and used for behavioral advertising."[90] The icon will also signal that a company engages in behavioral advertising and abides by the Industry Program's principles. When a consumer clicks on the icon, they will be linked to "a 'clear' disclosure statement regarding the company's data-collection practices, as well as an 'easy-to-use' opt-out option."[91] Critics urge that the Industry Program and other self-regulatory principles, "don't protect consumers, haven't worked before, and are largely designed for no reason except to take the congressional eye off the reform ball."[92] Also, companies have little incentive to commit to self-regulatory principles like the Industry Program because, "[a] company that agrees to comply with the program and fails to do so could be found in violation of Section 5 of the FTC Act" prohibiting "unfair and deceptive trade practices."[93] After all, when a company has not made an affirmative statement, "[it is] more difficult to bring a deception claim."[94] Thus, companies face fewer risks if they do not make an affirmative statement like the one required by the Industry Program.

2. THE FTC'S PROPOSED FRAMEWORK OF 2010

Answering the call for additional protections, the FTC published a Preliminary FTC Staff Report proposing a framework to better protect consumer information, noting that the "notice-and-choice model, as

---

[90] Alexei Alexis, *Marketing: Web Marketers Launch Self-Regulatory Plan with Opt-Out for Behavioral Data Collection*, 9 PRIVACY & SECURITY L. REP. NO. 40 (BNA), at 1385–86 (Oct. 11, 2010).

[91] *Id.*

[92] *Id.*

[93] *See, e.g.*, Bick, *supra* note 24 (While the FTC has allowed online consumer data collection to be self-regulated, "the agency has prosecuted Web-site owners who fail to disclose behavioral-targeting techniques in a clear and conspicuous manner." For example, the FTC brought an action against Sears Holdings Management Corporation because "Sears obscured the extent of the data collection, which included health, banking and other sensitive data, in its privacy statements."); *see also* In the Matter of Sears Holdings Mgt. Corp. C-4264 (F.T.C. Aug. 31, 2009).

[94] Alexis, *supra* note 90.

implemented [thus far], has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[95] The framework makes four core recommendations: (1) The framework suggests that it apply to both online and offline commercial entities that gather and use data that can be "reasonably linked to a specific consumer, computer, or other device."[96] (2) Companies should integrate consumer privacy measures throughout their organization and at each stage in the development of new products and services.[97] When data is collected for "commonly accepted practices," consumer choice is not required. But for other purposes, the company should offer the consumer a clear choice of whether or not to provide the data.[98] (3) Companies should create clear, understandable, and uniform privacy notices. Companies should allow consumers to access the data that has been collected and retained about them. (4) If a company chooses to use consumer data in a way that is "materially different" from its stated purpose when it collected the data, it should do so only after obtaining express permission from the consumer.[99]

The FTC also recommended the development of a "do not track" system[100]—a "simple, easy to use choice mechanism for consumers to opt out of the collection of information about their Internet behavior for targeted ads."[101] The idea for a do-not-track system similar to the

---

[95] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, iii (2010) [hereinafter FTC PROPOSED FRAMEWORK 2010].

[96] *Id.* at v. This scope demonstrates the FTC's recognition that "the distinction between data containing personally identifiable information and anonymous data is becoming less meaningful." Julia Angwin & Jennifer Valentino-Devries, *FTC Backs Do-Not-Track System for Web*, WALL ST. J., Dec. 2, 2010, http://online.wsj.com/article/SB10001424052748704594804575648670826747094.html.

[97] FTC PROPOSED FRAMEWORK 2010, *supra* note 95, at 40.

[98] *Id.* at 20–28. These commonly accepted practices include, "product and service fulfillment," internal operations," fraud prevention," "legal compliance and public purpose," and "first-party marketing," for example, where online companies recommend products based upon a consumer's previous purchases on that company's website. *Id.* at 53–54.

[99] *Id.* at 41–42.

[100] *Id.* at 66–69.

[101] Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), http://www.ftc.gov/opa/2010/12/privacyreport.shtm.

"Do Not Call" registry prohibiting telemarketing telephone calls was first raised in 2007. However, the difficulty of implementing such a system prevented its creation.[102] New technologies may now make a do-not-track system possible. Privacy researchers believe it is possible to install a small piece of code in web browsers that would "broadcast a message to every website saying 'do not track this user.'"[103]

The FTC report requested comments on its current framework[104] and a final version of the framework is forthcoming.[105] However, this new FTC framework remains "recommendations for best practices" and not regulations "for enforcement."[106]

B. THE ABSENCE OF CONGRESSIONAL LEGISLATION

There remains no federal online tracking regulation, and it seems unlikely that Congress will enact comprehensive online privacy regulations in the near future. Congress entered the online consumer tracking debate in 2010.[107] In May, 2010, Representative Rick Boucher, Chair of the Subcommittee on Communications, Technology, and the Internet, circulated a draft legislative proposal of a comprehensive federal privacy regulation that would have imposed new restrictions on the collection and use of consumer data.[108] Representative Boucher's proposed legislation applied broadly—to "any entity engaged in interstate commerce that collects covered information, such as a person's name, postal and e-mail address, telephone number, 'preference profile,' or 'unique persistent identifier,' such as an Internet protocol address."[109] The legislation

---

[102] Julia Angwin & Spencer E. Ante, *Hiding Online Footprints*, WALL ST. J., Nov. 30, 2010, http://online.wsj.com/article/SB10001424052748704584804575645074178700984.html?mod=WSJ_Tech_LEFTTopNews.

[103] *Id.* The proposal of a do-not-track system was met with immediate criticism. *See infra* notes 109–113 and accompanying text.

[104] FTC PROPOSED FRAMEWORK 2010, *supra* note 95, at 38.

[105] Angwin & Valentino-Devries, *supra* note 96.

[106] *Id.* (quoting FTC Commissioner Jon Leibowitz).

[107] Daniel T. Rockey, *Proposed Data Privacy Legislation Generates Relief as Well as Concerns*, 9 PRIVACY & SEC. L. REP.(BNA), at 961 (June 28, 2010).

[108] Alexis, *supra* note 88.

[109] *Id.*

mandated a "clear, understandable privacy policy explaining how [covered information] is collected, used, and disclosed," and required consumer opt-in for the use of any "sensitive data, such as medical records, financial accounts, Social Security numbers, and location information," and offered limited exceptions to these mandates.[110] The bill also required that companies "delete or 'render anonymous' any covered information" eighteen months after collection.[111] This proposed legislation faced criticism from both the industry, concerned about how disruptive the regulation would be to current business models, and consumer advocacy groups, arguing that the proposal does not impose enough restrictions to adequately protect consumers.[112] Online privacy regulations require an informed, delicate balancing of interests.[113] The proposed privacy regulations may have left room for improvement, but it appears that the bill did not advance far beyond the proposal stage. Representative Boucher was defeated in the November 2010 elections, and his absence likely had a debilitating impact on the bill's legislative progress.[114]

Congress revived the idea of a do-not-track system in February 2011 when it began considering the "Do Not Track Me Online Act of 2011."[115] If passed, this legislation would give the FTC eighteen

---

[110] *Id.* (noting that the opt-in mandate was "just one of many areas of the proposal that are expected to generate debate").

[111] *Id.* For a discussion cautioning against this type of reliance on "anonymization" in privacy statutes and regulation, see *supra* notes 67–68 and accompanying text.

[112] *Id.* ("With only limited exemptions included, the proposal would leave many data-sharing arrangements—as they exist today—in legal jeopardy." Still, consumer advocacy groups have "argued that his proposal does not go far enough.").

[113] *See* Andrea N. Person, Note, *Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May be Limiting the Online Experience*, 62 FED. COMM. L.J. 435, 437 (2010) ("While protecting the personal information of Americans online should be a top priority, it is equally important to consider how regulation in this area may affect the future of the Internet and how too much regulation may harm the consumer.").

[114] Mike Shields, *Online Privacy Bill: Dead in the Water?*, ADWEEK (Nov. 4, 2010), http://www.adweek.com/aw/content_display/news/politics/e3if13877e698a1cce2faa1baf6cc66750a.

[115] *Speier Introduces Consumer Privacy Package* (Feb. 11, 2011), http://speier.house.gov/index.php?option=com_content&view=article&id=215:speier-introduces-consumer-privacy-package&catid=1:press-releases&Itemid=14; *see also* David Sarno, *"Do Not Track" Internet Privacy Bill Introduced In House*, L.A. TIMES, Feb. 11, 2011, http://www.latimes.com/business/la-fi-do-not-track-20110212,0,66573.story.

months to create regulations requiring advertisers to "allow users to 'effectively and easily' choose not to have their online behavior tracked or recorded."[116] However, such a system could dramatically decrease the availability of free content,[117] and the implementation of a do not track mechanism remains difficult; browser makers must build the feature and "[i]t would only work if tracking companies would agree to honor the user's request."[118] Reflecting these concerns, the bill was met with immediate criticism from the industry, including the charge that the do not track program Congress envisions "would require re-engineering the Internet's architecture," resulting in a "severely diminished experience" for consumers.[119] As of this publication, the bill remains in the beginning stages of lawmaking, with the last related action being its referral to the House Subcommittee on Commerce, Manufacturing, and Trade one week after it was introduced in February 2011.[120]

V. THE REGULATION CHALLENGE: BALANCING OPTIONS

Consumers, governments, and companies around the world are searching for a suitable approach to online consumer tracking and behavioral advertising. Any regulation or system must address consumer privacy issues without eliminating the functionality and benefits that the Internet and its industry provide. Innovative

---

[116] Sarno, *supra* note 115.

[117] Angwin & Valentino-Devries, *supra* note 96 ("'FTC endorses 'do not track'; an emotional goodbye to free content so kindly funded by advertisers,' tweeted Rob Norman, chief executive of WPP PLC's GroupM North America, which buys ads on behalf of corporate clients.").

[118] *Id.* (Mozilla Corp.'s Firefox Web browser explored a built-in do-not-track mechanism but chose not to include the tool in its browser, fearing that such a tool "would force advertisers to use even sneakier techniques and could slow down the performance of some websites.").

[119] Grant Gross, *Lawmaker Introduces Online Do-Not-Track Bill*, PCWORLD (Feb. 11, 2011, 4:32 PM), http://www.pcworld.com/businesscenter/article/219454/lawmaker_introduces_online_donottrack_bill.html ("Do Not Track" as a method of protecting consumers "resonate[s] with the public," but practically, it remains "difficult to implement.").

[120] Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011).

solutions have been explored but no one method has proven a completely successful approach.

A. A MISSION THAT WON'T SELF-DESTRUCT: PREVENTING THE HARM WITHOUT REGULATING AWAY THE BENEFITS

Tracking has strengthened the behavioral advertising industry and consumers have grown fond of the benefits that such paid advertising provides, which adds to the challenge of creating regulations. Targeted ads show consumers advertisements that will likely interest them. The benefits of targeted advertising also include Internet features that many consumers have come to expect since targeted ads fund much of the website content that consumers access free of charge.[121]

Several tracking methods use technology that is also used for fraud protection. Both "evercookies" and device fingerprinting are essential tools for fraud protection. If device fingerprinting and evercookies are banned, that could have grave consequences for the Web and the way it functions.[122] In fact, if these techniques for identifying fraudsters were prohibited or blocked by Web browsers "it would essentially make it impossible to shop over the internet."[123] Regulation to protect consumer privacy could ban technologies that provide benefits to consumers and inhibit Web functions we all rely upon.[124]

B. THE EUROPEAN UNION'S STRUGGLE WITH OPT-IN

---

[121] Richard M. Marsh, Jr., Note, *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 MICH. TELECOMM. & TECH. L. REV. 543, 544 (2009).

[122] Valentino-Devries, *supra* note 38.

[123] *Id.* The elimination of cookies also impacts the way many websites function. Edwards & Hatcher, *supra* note 10, at 3. (Amazon's website "(unusually) provides fairly good functionality without cookies, but popular features such as the 'shopping cart' and 'your preferences' do disappear. Many sites however simply fall over if the user chooses to 'turn off' or delete" the cookies for that site." Similarly, search engines collect and store search data for business purposes that benefit consumers); *see also* Edwards & Hatcher, *supra* note 10, at 14 (Search engines like Google collect data in order "to improve their own search algorithms" which allow the tailored and accurate searches Internet users appreciate and expect).

[124] *See, e.g.*, *supra* Part II.B.4.

The European Union (EU) leads the world in the area of online privacy law.[125] But, the EU, like the United States, is struggling to find the best method of regulating the collection and use of consumer information online.[126] The EU's recent attempt at implementing an opt-in requirement for online consumer tracking is a cautionary tale.[127] Previously, European law required websites to allow consumers to "opt out" or refuse cookies. But in 2009 the EU passed a law requiring companies to "obtain consent from Web users when tracking files such as cookies are placed on users' computers."[128] As the law waited for enactment by member countries, a dispute over its meaning erupted and "Internet companies, advertisers, lawmakers, privacy advocates and EU member nations" became entangled in debate over what the law actually requires in practice.[129] If a user agrees to cookies when setting up her Web browser, is that a sufficient opt-in? If an industry plan allows users to see and opt out of data that has been collected about them, is that sufficient consent? Must a consumer "check a box each time" before a cookie may be placed on his machine?[130] The law has now passed, but the dispute over its meaning continues with no clear answer in sight and no change in the way cookies are used for tracking. The EU's approach to online privacy regulation demonstrates just how difficult it is to regulate the practice of tracking Internet users' behavior on the Web, and lawmakers must carefully consider the impact and implementation of any requirement.[131]

---

[125] *See, e.g.*, Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 116–17 (2002) (comparing the EU's "comprehensive" privacy legislation—the Data Protection Directive—with the United States' "ad hoc" approach to information privacy in general).

[126] *See* Kuneva, *EU Consumer Comm'r*, *supra* note 10.

[127] Paul Sonne & John W. Miller, *EU Chews on Web Cookies*, WALL ST. J., Nov. 22, 2010, http://online.wsj.com/article/SB10001424052748704444304575628610624607130.html?mod=WSJ_Tech_LEADTop.

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

C. CONSUMER OPT-OUT TOOLS IN THE U.S.

Consumer opt-out tools have also emerged in the United States. Using various methods, these tools allow consumers to opt-out of some behavioral advertising.

Both the Self-Regulatory Program for Online Behavioral Advertising and the Network Advertising Initiative (NAI) have instituted consumer opt-out web pages which allow users to decide whether or not they receive interest-based advertising from companies participating in each program. The websites show consumers which participating advertisers have been tracking them and delivering behavioral or "interest-based" advertising targeted to them. Consumers can choose to opt-out of interest-based advertising from those participating advertisers.[132] However, these opt-out selections are stored in "opt-out cookies." This means that consumers' opt-out selections will be erased any time they clear their cookies. Also, the consumers' opt outs only prevent interest-based advertising; consumers will still receive non-interest-based advertising, and thus will continue to be tracked.[133]

D. GOOGLE'S PRACTICAL OPT-OUT SOLUTION

Google's online privacy program, its "Ad Preference Manager," also supports a consumer opt-out rather than an opt-in, system. For years Google had struggled to determine how far it was willing to go to profit from its "crown jewels," "the vast trove of data it possesses about people's [online] activities."[134] As a leader in the industry, "[f]ew online companies have the potential to know as much about its users as Google."[135] Google has access to the information users store in Google Docs, its online word processor and spreadsheet; it also has access to all of the emails users send through Gmail and it saves the

---

[132] *See Opt Out from Online Behavioral Advertising (Beta)*, ABOUTADS, http://www.aboutads.info/choices (last visited Sept. 10, 2011); *Opt Out of Behavioral Advertising*, NETWORK ADVER. INITIATIVE, http://www.networkadvertising.org/managing/opt_out.asp (last visited Sept. 10, 2011).

[133] *See Opt out of Behavioral Advertising*, *supra* note 132.

[134] Vascellaro, *supra* note 15.

[135] *Id.*

searches those same users execute, making the search data anonymous after eighteen months. However, when it came to using this user data, the company initially held back, concerned about privacy issues. Google makes its money selling ads—originally, "ads tied to the search-engine terms people use."[136] Google's policies allowed only display ads based on "contextual" targeting (putting a shoe ad on a page about shoes). As the industry changed and advertisers became interested in targeting consumers "based on more specific personal information such as hobbies, income, illnesses or circles of friends," Google has been forced to change too.[137] In 2007 Google purchased DoubleClick, a "giant" in the online advertising business. Google executives remained reluctant to use cookies to track people online, because many users were unaware that they were being tracked. Finally, in March 2009, Google did launch an interest-based ads product that uses cookies to track a user's visits to "one of the more than one million sites where Google sells display ads."[138]

However, Google "elegantly" and simply addresses the many practical problems of implementing notice and choice regarding its consumer tracking with its ad preference manager.[139] Google's approach has proven functional while still promoting transparency and consumer control. Further, it presents a privacy solution that has been called "superior" to a do-not-track system.[140] Google tracks users' browsing activity across sites using AdSense and creates a profile of each user's interests. Like many advertisers, Google uses this profile to

---

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] Berin Szoka, *Google's Ad Preference Manager: One Small Step for Google, One Giant Leap for Privacy*, THE PROGRESS & FREEDOM FOUND., Mar. 2009, *available at* http://ssrn.com/abstract=1421876; *see also* Jennifer Valentino-Devries, *What They Know About You*, WALL ST. J., July 31, 2010, http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html (Google, the most prevalent tracker in the nation's forty-nine of the fifty Web sites, as tested in a recent *Wall Street Journal* survey, does allow consumers to use Google's Ads Preferences Manager, at http://www.google.com/ads/preferences, to "see the name of the tracking file, or 'cookie,' it associates with [their] Web browser and the interests it links to that cookie." Google's manager "lets [consumers] remove some interests and add others, choosing from a list ranging from 'poetry' to 'neuroscience' to 'polar regions.'" A consumer can also chose to opt-out so Google will no longer track him.).

[140] *See* Szoka, *supra* note 139, at 3.

tailor the ads delivered on the Google Content Network (GNC) and YouTube.[141]

Through its Ad Preference Manager, Google provides notice of its tracking to consumers in two ways. First, each ad notifies the user which advertiser is paying for the ad and that Google is serving it. The bottom left-hand corner of "each AdSense ad on sites in the GNC" contains the URL of the advertiser's website. In the bottom right-hand corner of the ad, an "Ads by Google" link will be displayed. Second, the "Ads by Google" link leads a user to his or her profile with the categories and subcategories that have been assigned to the tracking cookie in his or her browser.

Google also provides choice to consumers in two ways. The Ad Preference Manager allows users to both view and edit the profile that has been assembled based on tracking. Consumers can select or delete categories of interests in their profiles. In addition, users have the ability "to opt-out completely from having their data collected" for behavioral advertising purposes, a choice that "will be respected in the future and will therefore be 'persistent.'"[142] Google's Ad Preference Manager addresses privacy advocates' concerns that opt-out systems make it too difficult for consumers to find the tool to opt-out and do not provide a "persistent" opt-out, requiring "the placement of a special 'opt-out cookie' on the user's computer, which may be inadvertently deleted when users delete all their cookies."[143] Such "user empowerment tools" have proven effective in similar contexts such as "online child protection, where parental control software offers a more effective alternative to government regulation of Internet content."[144] Google's approach allows for flexibility, as it does not absolutely block ad companies' abilities to track and target. Such practices fund free online content and allow fraud prevention mechanisms to operate.[145] Google's approach is not a flawless model and could not be widely implemented. There are countless different companies advertising and collecting consumer data on the Internet, all around the world. If each advertising company on the Internet

---

[141] *Id.* at 1.

[142] *Id.* at 2.

[143] *Id.* at 3.

[144] *Id.* at 4; *see also* Children's Online Privacy Protection Rule, 16 CFR § 312 (2010).

[145] *See* Szoka, *supra* note 139, at 6. For examples of potential negatives effects of a ban on tracking, see *supra* notes 111, 116–18, and accompanying text.

provided this tool, the result would be a complex and time-consuming system requiring consumers to monitor and manage all of their individual profiles for each and every company. Also, because tracking and targeting are not fully prohibited with Google's method, some privacy issues are left unaddressed.

VI. CONCLUSION

Unregulated online consumer tracking and collection of consumer data present significant privacy issues. While the self-regulation and best-practices models the FTC has used thus far allow the industry a great deal of power to innovate, there remains little incentive for companies to fully participate.[146] Much debate has centered on which government entity—Congress,[147] the FTC,[148] the Department of Commerce,[149] or a White House Task Force[150]—should govern consumer tracking and whether regulation should take the form of recommendations for self-regulation or stringent law.

Various methods for addressing the privacy issues surrounding online tracking have been implemented by regulators and companies, but none has proven to be an ideal model. Although a consumer ad management tool such as Google's resolves many of the practical issues and provides a great deal of user control, it is not a system that could be widely implemented. There remains no clear solution to the privacy issues surrounding online tracking and behavioral advertising. However, it is apparent that any regulation of online consumer tracking and behavioral advertising should strike a delicate balance. Regulation must provide adequate protections to consumers and its scope must encompass a broad range of ever-developing techniques

---

[146] *See supra* Part IV.A.

[147] *See supra* Part IV.B.

[148] *See supra* Part IV.A; *see also* FTC PROPOSED FRAMEWORK 2010, *supra* note 95; FTC STAFF REPORT 2009, *supra* note 85.

[149] *See* THE U.S. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

[150] *See* Julia Angwin, *Watchdog Planned for Online Privacy*, WALL ST. J., Nov. 11, 2010, http://online.wsj.com/article/SB10001424052748703848204575608970171176014.html ("[T]he White House has created a special task force that is expected to help transform the Commerce Department recommendations [on policing Internet privacy] into policy.").

used to track. At the same time, regulation should not stifle the innovation through which the Internet has developed and thrived, and must not regulate to the point of eliminating the functionality of the Web.