Chicago-Kent Journal of Intellectual Property

Volume 13 | Issue 2 Article 9

7-1-2014

Online Tracking: Can the Free Market Create Choice Where None Exists?

Benjamin Strauss

ONLINE TRACKING: CAN THE FREE MARKET CREATE CHOICE WHERE NONE EXISTS?

Benjamin Strauss[*]

INTRODUCTION

Our online privacy is compromised every time we surf the World Wide Web. The individual privacy of online users is quickly eroded by hackers, Internet advertisers, and other online entities. Behavioral advertisers are tracking our every move, cataloguing our user data, and selling it to the highest bidder. Advertisers use that information to infer users' most sensitive interests to inundate them with ads specifically targeted to their web browsing history. Consumers are often presented with boilerplate privacy policies that they must consent to prior to using a web service or mobile application (app). Consumers have no means to fight back. They can either consent to data collection, or forego using the online service. As we live more and more of our lives online, this is nothing more than a Hobson's choice.

In Part I of this Note, I hope to shed light on the many privacy problems faced by users each time they browse the web. I then turn to current strategies aimed at combatting these global problems. In Part II, I highlight international approaches taken to protect online privacy. First, I detail the European Union's approach to combatting many of these problems. The European Union has the most comprehensive online privacy regime, and can serve as a useful guide to our legislature in the future. I also highlight China's approach to online privacy and its recent attempts to establish baseline Internet security standards.

In Part III, I turn to the United States' futile endeavor to protect online privacy. Although presented with numerous proposals, Congress has failed to pass any significant legislation addressing online privacy issues. I outline several recent proposals and analyze their potential effectiveness. Next, I turn from federal legislation to state legislation and detail California's attempt to implement privacy protections for its citizens in an area where the federal government has failed to act.

In Part IV, I propose a practical solution. Any privacy protection regime should place power in the hands of consumers. Consumers should have notice as to what information is collected about them, and have some enforceable mechanisms to opt out of Internet tracking. Federal legislation is one way to address this problem, but many believe it is unlikely the government can keep

---

 UCLA School of Law, Class of 2014. Sincere thanks to Professor Curt Hessler for his Digital Wars seminar and to the editorial staff of the *Chicago-Kent Journal of Intellectual Property*.

up with the innovative and vibrant pace of the Internet. The free market offers alternatives. A voluntary Do-Not-Track system could potentially be effective in the future. Any mechanism for consumers to opt out must be comprehensive, effective, and simple. By placing this power in the hands of consumers, we can force advertisers to reform their data collection practices to better respond to consumer preference and national consensus.

I. THE PROBLEM(S)

The *Wall Street Journal* has performed the most extensive research on the problems presented by online tracking.[1] In this section, I detail several problems that every Internet user faces as they surf the World Wide Web.

A. First- and Third-Party Cookies

Cookies are small text files containing a string of numbers that websites can use to identify you.[2] Websites use cookies to store information about you when you visit the website.[3] Advertisers can also access this cookie and track how you navigate the Internet. There are two types of traditional HTTP cookies: first-party cookies and third-party cookies. First-party cookies are issued by the host website or the website you are currently accessing[4] to keep track of activity as you move throughout that single website. Without first-party cookies, a website could not keep track of your activity as you move from page to page. For example, it would be impossible to purchase multiple items in the same transaction because each time you added something to the cart from another page on the site, it would be treated as a new order.[5]

First-party cookies also make browsing the web more convenient. Cookies allow websites to remember your username and password so you don't need to sign in every time you access a site. Cookies can also track preferences to show the user more websites that might interest them. However, cookies carry risks as well. Hackers can obtain your username and password from the cookie file saved on your computer.[6] Additionally, programs such as Opentracker offer

---

[1] *See generally What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Apr. 18, 2014).

[2] Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 276 (2012).

[3] *Id.*

[4] *Id.*

[5] *See* Jay P. Kesan & Rajiv C. Shah, *Deconstructing Code*, 6 YALE J.L. & TECH. 277, 298–99 (2004).

[6] *See, e.g.*, Julie Bort, *2 Million More Passwords for Facebook, Google, Twitter, Other Sites Were Stolen and Posted to the Net*, BUSINESS INSIDER (Dec. 4, 2013, 2:10 PM), http://www.businessinsider.com/2-million-more-passwords-stolen-2013-12.

services to web hosts to track users who access their site.[7] By using this type of software, web hosts can track information about their visitors such as search terms, geographical location, and all pages viewed during a browsing session.[8]

Third-party cookies, on the other hand, are issued by websites other than the host website. These cookies are "commonly used to track users across different websites by companies that have no relationship with consumers."[9] These websites are typically advertisers, tracking companies, and other web analytics service providers.

The cookie privacy problem presents itself in the aggregation of tracking from all these cookies across many different websites.[10] Companies tracking these cookies can aggregate this browsing information into profiles and even link these profiles to users' identities.[11] The process of profiling (also known as "tracking") assembles and analyzes several events, each attributable to a single user, in order to gain information (especially patterns of activity) relating to this user. Through profiling, advertisers can infer users' interests, including sensitive ones such as "medical conditions, political opinions, or even sexual fetishes."[12]

This form of profiling becomes most contentious when data-matching software associates the aggregated profile of a user with personally-identifiable information of the actual individual such as their name, address, or telephone number. It is one thing for advertisers to have an aggregated browsing profile linked to an IP address, but it is another to link a name and face to a browsing history. This can occur when users sign up for web services and fill out sign-up forms with their personal information.[13] Advertisers can then link the personal information provided by the user to the existing cookies on that computer.[14] This creates a link between the user's true identity, and his or her identifying cookie and the associated data profile.

B. Breaking the Link

Deleting third-party cookies has become a convenient option for privacy-sensitive users. By deleting their cookies, consumers can avoid some online tracking.[15] The most prominent web browsers (Chrome, Firefox, and Internet Explorer) have this capability built-in. Users can manually delete all cookies by

---

[7] *Track Unique Visitors*, OPENTRACKER, http://www.opentracker.net/products/web-analytics/feature/track-unique-visitors (last visited June 16, 2014).
[8] *Id.*
[9] Hoofnagle et al., *supra* note 2, at 276.
[10] *Id.*
[11] *Id.* at 276–77.
[12] *Id.* at 276.
[13] *Id.*
[14] *Id.* at 276–77.
[15] *Id.* at 277.

navigating the web browser's preferences.[16] Additionally, most web browsers offer the option to automatically clear cookies each time the user closes the web browser.[17]

Deleting cookies breaks the link between "the identifier assigned to [his or] her computer and the tracking mechanisms on the advertisers' servers."[18] Once deleted, the server will assume that a new person is visiting the website and assign a new cookie to the device.[19] While deleting cookies may prevent potential privacy risks, it will also likely limit or prevent the functionality of many websites. Deleting cookies eliminates the benefits of cookies discussed above, making the web-browsing experience less enjoyable and more burdensome. While this is one tool in the fight against tracking, advertisers have other means at their disposal.

C. The Unbreakable Link

"Flash cookies," or "local shared objects," are files used by Adobe Flash developers to store data on users' computers.[20] Adobe argues that local shared objects allow Flash developers and websites to "create richer and more personalized user experiences" by providing a "more customized experience."[21] Traditionally these Flash cookies are used to store useful data such as volume settings for Internet videos and other user preferences.[22] They can also make navigating the Internet more convenient by storing usernames, passwords, and other information to "auto-fill" forms.[23] However, they can also be used to store unique identifiers for tracking users in the same way as traditional HTTP first- and third-party cookies.[24]

Most problematic is the fact that Flash cookies possess the capacity to "circumvent cookie deletion."[25] The option in most browsers to reject or delete cookies does not affect Flash cookies.[26] Flash enables "respawning" of

---

[16] *See* Scott Orgera, *How to Delete Cookies*, ABOUT.COM, http://browsers.about.com/od/faq/tp/delete-cookies.htm (last visited June 16, 2014).

[17] Hoofnagel et al., *supra* note 2, at 277–78.

[18] *Id.* at 278.

[19] *Id.*

[20] *What is a Local Shared Object?*, ADOBE, https://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-flash.html (last visited June 16, 2014).

[21] *Id.*

[22] Hoofnagle et al., *supra* note 2, at 277.

[23] *What is a Local Shared Object?*, ADOBE, https://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-flash.html (last visited June 16, 2014).

[24] Hoofnagle et al., *supra* note 2, at 277.

[25] *Id.* at 278.

[26] Nurie Mohamed, *You Deleted Your Cookies? Think Again*, WIRED (Aug. 10, 2009, 7:39 PM), http://www.wired.com/business/2009/08/you-deleted-your-cookies-think-again/.

cookies.[27] Certain websites use Flash cookies to restore first- and third-party browser cookies that users have previously deleted.[28] Essentially Flash cookies link the new cookie with the old and re-enable continuous tracking between websites.[29] Flash cookies also possess far more storage capacity than traditional first- and third-party cookies. The traditional HTTP cookie can store a maximum of 4 kilobytes of information.[30] Flash cookies, on the other hand, store one hundred kilobytes of data by default and possess an unlimited maximum.[31] This opens the door to far more detailed profiling of users as more and more information is logged and stored by Flash cookies.

According to Adobe's Chief Privacy Officer, Meme Jacobs Rasmussen, Flash cookie use appears to be waning due to market forces, specifically consumer backlash about their use.[32] Adobe took substantial criticism for the exploitation of their Flash cookies, and claims they are currently working to provide better privacy protections for Adobe users.[33] Adobe even participated in industry discussions on the topic and submitted an official comment to the Federal Trade Commission (FTC) confirming their "commitment to supporting research into the types and extent of the misuse of local storage."[34]

While the use of Flash cookies appears to be waning, Internet innovation will likely create new ways in which advertisers can circumvent cookie deletion. There has been a rise in the use of HTML5 cookies which possess many of the same characteristics of flash cookies, and can store five megabytes of data. Any solution to protect online privacy must not only cover current technology, but must also be adaptive to anticipate and address future innovations by advertisers and tracking companies.

---

[27] Hoofnagle et al., *supra* note 2, at 278.

[28] *Id.*; Antone Gonsalves, *Company Bypasses Cookie-Deleting Consumers*, INFORMATIONWEEK (Mar. 31, 2005, 5:14 PM), http://www.informationweek.com/company-bypasses-cookie-deleting-consumers/d/d-id/1031518?.

[29] Hoofnagle et al., *supra* note 2, at 278.

[30] *Id.* at 277.

[31] *Id.*

[32] Meme Jacobs Rasmussen, *Carnegie Mellon University Study Suggests Browser Cookie Respawning May Be Waning*, ADOBE FEATURED BLOGS (Jan. 31, 2011, 8:30 AM), http://blogs.adobe.com/conversations/2011/01/carnegie-mellon-university-study-suggests-browser-cookie-respawning-may-be-waning.html.

[33] *Id.*

[34] Comments from Adobe Systems Incorporated – Privacy Roundtables Project No. P095416 1 (Jan. 27, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00085/544506-00085.pdf.

D. Mobile Apps

With the surge in popularity of the Apple's "App Store" and the Google Play Store, cookies are becoming less effective in tracking mobile users' activities. Cookies operate with respect to web browsers, but mobile devices do not require a web browser. Instead, individuals navigate the Internet through various mobile applications or "apps." However, these apps often include blanket agreements to track, store, and transfer all information shared through the app.[35] Mobile tracking presents new privacy problems, including the added component of geographic tracking.[36] Data collectors cannot only gather personal information about you, but can even determine where you are located (assuming you have your mobile device with you) at any given moment.[37] If you update your status on Facebook or tweet what you are doing on Twitter, advertisers now have information of where you are and what you are doing.

In many cases, apps want all or nothing as far as information goes. They require users to grant a blanket request for permissions that may include access to location data and contacts, or they simply will not run.[38] In a recent case in February 2012, a developer named Arun Thampi discovered that the iOS app for the social network "Path" was uploading his entire address book back to Path's servers without user permission.[39] Path automatically collected and stored personal information from the user's mobile address book even if the user did

---

[35] *See, e.g.*, Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building A Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 261 (2012). In June 2010, Apple made changes to its privacy policy indicating that Apple was sharing geographic location data of people who were using iPads, iPhones, and other Apple products. *Id.*

[36] Jonathan Carson, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NIELSON (Apr. 21, 2011), http://www.nielsen.com/us/en/newswire/2011/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location.html.

[37] *Id.*

[38] *See* Sarah Perez, *FTC Finds Privacy Problems in Children's Apps, but Suggested Changes Will Impact All*, TECHCRUNCH (Feb. 16, 2012), http://techcrunch.com/2012/02/16/ftc-finds-privacy-problems-in-childrens-apps-but-suggested-changes-will-impact-all/.

[39] Ben Weitzenkorn, *2 Congressional Bills Seek to Strengthen Online Privacy*, NBCNEWS.COM (Sept. 13, 2012, 4:50 PM), http://www.nbcnews.com/id/49024427/ns/technology_and_science-security/t/congressional-bills-seek-strengthen-online-privacy/#.U6Kh_xYsywI; Tomio Geron, *Path Apologizes for Contact Uploads, Deletes Data*, FORBES (Feb. 8, 2012, 6:18 PM), http://www.forbes.com/sites/tomiogeron/2012/02/08/path-apologizes-for-contact-uploads-deletes-data/.

not "opt in" to the "Find friends from your contacts" option.[40] This practice led to an $800,000 fine from the FTC for violating the Children's Online Privacy Protection Act of 1998.[41] The company subsequently apologized, deleted the data, and updated the app to request permission before collecting any data.[42] It is unclear if this actually worked because a year later, in April 2013, users reported that Path sent spam text messages to their contacts. Stephen Kenwright described on his blog how the app texted his parents, grandparents, and an aunt to tell them he "had a photo to share with them."[43]

The market will likely flush Path's invasive practices out. Fewer and fewer people will wish to sign up for an application that does not take measures to secure personal data. There have been several attempts to regulate these apps including Senator Edward Markey's proposed Mobile Device Privacy Act.[44] This bill, and other non-market-based solutions, is discussed below in Part III.

E. Mobile Location Analytics

Brick-and-mortar stores are attempting to gather behavioral information about their customers as though they are an online retailer like Amazon.com. Earlier in 2013, several brick-and-mortar stores partnered with tracking companies to collect information about customer behavior based upon their movements around the store.[45] Mobile location analytic companies such as Brickstream,[46] Euclid,[47] and Nomi[48] offer tools for retailers to record information such as visit frequency and duration, walk-bys, repeat visitor ratio, and the path shoppers take as they move throughout the store.[49]

Companies such as Nordstom and Home Depot partnered with Euclid Analytics and implemented technology that allowed it to track customers' movements around the store by following the Wi-Fi signals emitted from their

---

[40] Press Release, Federal Trade Commission, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), http://www.ftc.gov/opa/2013/02/path.shtm.

[41] *Id.* For more information on COPPA, see *infra* Part III.A.2.

[42] Geron, *supra* note 39.

[43] Stephen Kenwright, *The Antisocial Network: Path Texts My Entire Phonebook at 6am*, BRANDED3 (Apr. 30, 2013, 1:56 PM), http://www.branded3.com/blogs/the-antisocial-network-path-texts-my-entire-phonebook-at-6am/.

[44] Mobile Device Privacy Act, H.R. 6377, 112th Cong. (2nd Sess. 2012).

[45] Brian Fung, *How Stores Use Your Phone's WiFi to Track Your Shopping Habits*, WASH. POST (Oct. 19, 2013, 11:32 AM), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/.

[46] BRICKSTEAM, http://www.brickstream.com/ (last visited June 16, 2014).

[47] EUCLID, http://euclidanalytics.com/ (last visited June 16, 2014).

[48] NOMI, http://www.getnomi.com/ (last visited June 16, 2014).

[49] *Euclid Metrics*, EUCLID ANALYTICS, http://euclidanalytics.com/product/ (last visited June 16, 2014).

smartphones, even when customers did not connect to the store's network.[50] This information, coupled with in-store video surveillance, allows retailers "to learn information as varied as their sex, how many minutes they spend in [each] aisle and how long they look at merchandise before buying it."[51]

Many retailers, including national chains such as Family Dollar, Cabela's, Benetton, and Warby Parker, are testing these technologies and using the resulting data to decide whether to change the store layout, how to shorten lines, and whether to offer customized coupons.[52] It also allows stores to follow their customers' shopping patterns in order to improve customer service and maximize profit by making sure they have enough employees in the store.[53] Bricksteam for example, tracks not only movement, but where people stop, "providing data points to correlate with sales."[54] Ralph Crabtree, Bricksteam's Chief Technical Officer, likened this practice to what online retailers do: "Watching where people go in a store is like watching how they looked at a second or third web page."[55]

Nomi, a New York-based mobile analytics company, is "literally bringing the Amazon experience into the store."[56] When a shopper downloads a retailer's app or provides an e-mail address when using in-store Wi-Fi, Nomi pulls up a profile of that customer.[57] These customer profiles contain the number of recent visits, what products that customer was looking at on the web site last night, and the customer's purchase history.[58] The store then has access to that profile and can cater the customer's shopping experience to that profile.[59] Nomi's President, Corey Capasso, described the experience as follows: "I walk into Macy's, Macy's knows that I just entered the store, and they're able to give me a

---

[50] Ryan Grenoble, *Euclid Analytics and Retailers: How Stores Like Nordstrom Track You Via Your Smartphone's Wi-Fi Signal*, HUFFINGTON POST (May 13, 2013, 9:54 PM), http://www.huffingtonpost.com/2013/05/08/euclid-analytics-nordstrom-retailers-tracking-smartphone_n_3237534.html.

[51] Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=1&.

[52] *Id.*

[53] Kent Erdahl, *Some Stores Can Track Your Every Movement Because of Your Cell Phone*, FOX31 DENVER (Nov. 22, 2013, 10:10 PM), http://kdvr.com/2013/11/22/some-stores-can-track-your-every-movement-because-of-your-cell-phone/; *Smart Store Privacy*, FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/issues/smart-stores/ (last visited June 16, 2014).

[54] BRICKSTEAM, http://www.brickstream.com/ (last accessed Apr. 6, 2014).

[55] Clifford & Hardy, *supra* note 51.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

personalized recommendation through my phone the moment I enter the store."[60] Once in the store, Nomi tracks the customer's movements via Wi-Fi.[61] Mr. Capasso even suggested that the software can specifically tailor coupons based on the information collected. "If I'm going and spending 20 minutes in the shoe section, that means I'm highly interested in buying a pair of shoes."[62] The store then might send a coupon for sneakers to that customer, just like Google Chrome will show an ad for the sneakers you searched for in a previous browsing session.[63]

This technology is just blossoming and could expand greatly in the future. For example, Synqera, a start-up based in St. Petersburg, Russia, sells software for checkout devices that can personalize marketing messages "based on a customer's gender, age and mood, measured by facial recognition."[64] Ekaterina Savchenko, the company's head of marketing, suggested that if "you are an angry man of 30, and it is Friday evening, it may offer you a bottle of whiskey."[65] Customers likely would not have a problem if sales associates were hyper-attentive and collected this data personally from their shoppers. It is perhaps the accumulation of all this data by computers that makes it increasingly eerie.

The simplest way to circumvent this type of tracking is to simply turn off your devices' wireless cards whenever you enter a store.[66] It might be safer to turn them off before you enter the mall because some retailers will grab your MAC address as you walk by the store.[67] Some analytics companies, including Nomi, offer an opt-out function on their web sites where you can enter your MAC address and state your desire not to be tracked.[68] However, you would have to do this for every device you carry with you.[69] Additionally, some retail analytics companies don't provide the opt-out feature. It also poses the additional problem of having to provide your device's MAC address in order to avoid them collecting it in the first place.

Mobile analytics companies and retailers have faced negative press in recent months as more people learn about the programs. According to Tara Darrow, a Nordstom spokeswoman, "As of May 8, [2013,] Nordstrom is no

---

[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *See id.*
[64] Noreen Seebacher, *Predictive Analytics, Passive Wi-Fi Tracking and Other Privacy Threats*, CMSWIRE (Nov. 12, 2013), http://www.cmswire.com/cms/customer-experience/predictive-analytics-passive-wifi-tracking-and-other-privacy-threats-023115.php.
[65] Clifford & Hardy, *supra* note 51.
[66] Fung, *supra* note 45.
[67] *Id.*
[68] *Id.*
[69] *Id.*

longer using Euclid for data collection in their stores."[70] After a public outcry, and in an effort to ease privacy concerns, the industry attempted to take steps towards self-regulation. U.S. Senator Charles Schumer, the Future of Privacy Forum, a Washington, D.C.-based think tank, and a group of location analytics companies[71] released a code of conduct to promote customer privacy and transparency for mobile location analytics.[72] The "Mobile Location Analytics Code of Conduct," establishes an opt-out system where users must enter the twelve-digit MAC addresses of each of their mobile devices' Bluetooth and Wi-Fi chips into a database.[73] The Future of Privacy Forum hopes to build a central "Do Not Call" list for MAC addresses that tracking companies will commit to honoring.[74] This again returns to the irony discussed above that customers must provide their MAC address simply to avoid retailers from collecting it in the first place.

Commentators argue that the Code of Conduct does not go nearly far enough.[75] The opt-out provision is not only counter-intuitive, but many customers are unaware of tracking in the first place, much less whether they should opt out of a particular store's tracking software.[76] The Code of Conduct depends on notice to the consumer, but the notice provisions are ineffective. The notice provisions depend on the retailers, which are not party to the agreement, to implement in-store signage providing notice of the tracking.[77] Unfortunately, retailers are presented with countervailing incentives. They have seen customers get upset about the tracking after seeing posted signs, so there is an incentive to make the signs less noticeable.[78]

Even more disconcerting, the Code proposes establishing a widely-adopted symbol to indicate that mobile location tracking is taking place, rather than plain language such as: "If you're carrying a mobile device, this establishment may be tracking your movement and location."[79] Commentators

---

[70] Grenoble, *supra* note 50.

[71] Including Euclid, Mexia Interactive, Radius Networks, Brickstream, Turnstyle Solutions, and SOLOMO.

[72] Emily Tabatabai, *Mobile Location Analytics Companies Agree to Code of Conduct*, ABA SECTION OF ANTITRUST LAW (Nov. 8, 2013), http://thesecuretimes.wordpress.com/2013/11/08/mobile-location-analytics-companies-agree-to-code-of-conduct/.

[73] *Id.*

[74] Fung, *supra* note 45.

[75] *See* Parker Higgins & Lee Tien, *Mobile Tracking Code of Conduct Falls Short of Protecting Consumers*, ELECTRONIC FRONTIER FOUNDATION (Oct. 26, 2013), https://www.eff.org/deeplinks/2013/10/mobile-tracking-code-conduct-falls-short-protecting-consumers.

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

liken this strategy to the "AdChoices" icon.[80] AdChoices allows people to configure whether they are shown targeted online ads.[81] That icon has been widely adopted by advertisers, but is virtually unknown among users.[82]

It is ironic that data-tracking strategies implemented by online retailers have leaked into traditional brick-and-mortar retailers. The public outcry against such "in-person" tracking has led to the first attempt at self-regulation of mobile location analytics. It will be interesting to see how the opt-out requirements work in practice. To be truly effective they will likely need to be simplified with substantial notice provisions making customers aware of tracking. The opt-out procedure should be simple, and it should apply universally to all stores and all personal devices. This should be accomplished without a central registry where users have to disclose their MAC addresses. I address these potential solutions in more detail in Parts III and IV below.

II. INTERNATIONAL STRATEGIES TO PROTECT ONLINE PRIVACY

A. European Union

The European Union has a complex and comprehensive regulatory framework to ensure protection of individual privacy. The Data Protection Directive (Directive)[83] attempts to strike a balance between individual privacy and the free movement of personal data within the European Union.[84] The Directive strictly regulates collection and use of personal data, and "demands that each Member State set up an independent national body responsible for the protection of [this] data."[85]

---

[80] *Id.*

[81] *See* ADCHOICES, http://www.youradchoices.com/ (last visited June 16, 2014).

[82] *Id.*; *see* Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay & Yang Wang, *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, Symposium On Usable Privacy and Security 2012 (July 13, 2012), *available at* http://cups.cs.cmu.edu/soups/2012/proceedings/a4_Ur.

[83] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT [hereinafter Directive 95/46/EC].

[84] *Protection of Personal Data*, Summaries of EU Legislation, EUROPA (Jan. 2, 2011), http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.

[85] *Id.*

1. Data Protection Directive (European Parliament and Council Directive 95/46/EC)

The European Union presents a very broad definition of "personal data." In Article 2 of the Directive, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject')."[86] An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity . . . ."[87] The Directive aims at and sets forth guidelines to determine when "data processing" is lawful. Data processing includes any operation performed upon data, including "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction . . . ."[88]

The European Union's Directive and regulatory framework focuses on several areas. The first focus is data quality. The data must be processed fairly and lawfully, and be collected only for specified and explicit purposes.[89] The next area of focus is legitimacy. Mainly, personal data may be processed if the data subject has unambiguously given his or her consent, or processing is necessitated by the public interest.[90] The Directive also outlines several forbidden categories of processing.[91] Member States shall prohibit data processing on any information that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[92] Three notable exceptions to this provision occur when explicit consent is obtained, when processing is necessary to protect vital interests of the data subject, and for purposes of preventative or diagnostic medicine.[93]

Essential provisions of the Directive place power in the hands of the consumer, also called the "data subject." Every data subject has the right to obtain from the "data controller" any information stored about them.[94] Article 12 provides that "without constraint at reasonable intervals and without excessive delay or expense," each data subject has the right to be informed when his

---

[86] Directive 95/46/EC, *supra* note 83, art. 2(a).
[87] *Id.*
[88] *Id.* art. 2(b).
[89] *Id.* art. 6.
[90] *Id.* art. 7.
[91] *Id.* art. 8.
[92] *Id.*
[93] *Id.*
[94] *Id.* art. 10–12.

personal data is being processed, and the purposes of that processing.[95] The "controller" (or data processor) must provide his or her name and address, the purpose of processing, the recipients of the data, and all other information required to "ensure the processing is fair."[96] Article 12 also provides for "rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive."[97] This right carries with it the controller's duty to notify any third parties with whom the data has been shared of any rectification, erasure, or blocking, unless impossible or it requires a "disproportionate effort."[98]

Arguably, the most important provisions of the Directive involve the data subject's "right to object," or to "opt out" of data collection for the purposes of "direct marketing." Under Article 14 of the Directive, data subjects have the right to object "on request and free of charge" to the processing of personal data relating to him which the "controller anticipates being processed for the purposes of direct marketing."[99] Additionally, data subjects have the right to be informed "before personal data [is] disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."[100] These provisions are perhaps the only way for subjects of data collection to prevent their information from being transmitted to third parties for advertising purposes.

2. Where the Directive Falls Short

The RAND Corporation has done an extensive review of the European Data Protection Directive.[101] The study revealed several weaknesses in the Directive, most notably its inability to effectively cope with problems relating to continued globalization and international data flows.[102] As with any Internet regulation, one sovereign is attempting to deal with a global Internet that has web hosts and data processors all over the world. According to RAND, the rules on data export and transfer to third countries are "outmoded," and the tools providing for transfer of data to third countries are "cumbersome."[103]

---

[95] *Id.* art. 10–12.
[96] *Id.* art. 10, 19.
[97] *Id.* art. 12.
[98] *Id.*
[99] *Id.* art. 14(b).
[100] *Id.*
[101] *See* NEIL ROBINSON, HANS GRAUX, MAARTEN BOTTERMAN & LORENZO VALERI, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE (May 2009), *available at* http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf.
[102] *Id.* at ix.
[103] *Id.* at 26.

The Directive terms countries outside the European Union as "third countries," and regulates data transmission to these third countries.[104] Processors may only transfer personal data to a third country if the third country in question "ensures an adequate level of protection" of that personal data.[105] Without an "adequate level of protection," certain alternative paths are available, such as the consent of the data subject or the adoption of certain standard contract clauses.[106] The RAND Corporation determined that this "adequacy rule" found little support and resulted in a "mechanism where only countries that follow the Directive strictly are considered to have an adequate protection regime."[107] Only five non-E.U. countries have been found to have adequate legal protection frameworks: Switzerland, Canada, Argentina, Guernsey, and the Isle of Man.[108] "China, India, Brazil, Japan and Russia, are not included, and the United States is only covered through the 'Safe Harbor' Privacy Principles."[109] However, the notion that data processors in E.U. member countries are supposed to succeed economically while being barred from these emerging markets and the United States is preposterous.

Additionally, the alternative mechanisms for transmission have yet to be tested. Very few data processors are willing to implement standard contract clauses that make them assume direct responsibility for ensuring the security of the transfer and any other related data transfers.[110] Most importantly, in the event of an unauthorized transmission, the European Union has no jurisdiction over these "third countries" and could likely do little to protect personal data once transferred.

Adapting to increasing globalization will continue to present issues. The European Union is currently working on addressing these issues and reforming the Directive with the General Data Protection Regulation (GDPR).[111] The European Commission first proposed the GDPR in 2012 "to do away with the current fragmentation and costly administrative burdens" associated with the

---

[104] *See* Directive 95/46/EC, *supra* note 83, art. 25.
[105] *Id.*
[106] ROBINSON, GRAUX, BOTTERMAN & VALERI, *supra* note 101, at 33.
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.* at 34–35.
[111] *The Proposed General Data Protection Regulation: The Consistency Mechanism Explained*, EUROPEAN COMMISSION (June 2, 2013), http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm.

Directive.[112] Adoption of the GDPR has been postponed until at least 2015, with implementation likely to follow two years after.[113]

Notwithstanding its flaws, the European Union has the most comprehensive data privacy regime in the world. The Directive can provide useful guidance to Congress as they attempt to implement legislation intended to protect online privacy. Congress should look to the effective provisions of the Directive, such as the "right to object," and continue to monitor the development of the GDPR.

B. China

Over the past few years, China has attempted to establish baseline Internet security standards to encourage consumer engagement in the Chinese e-commerce market.[114] In 2012, the National People's Congress passed a law regulating the collection and use of personal electronic information.[115] The Decision on Strengthening Protection of Online Information (Decision) governs businesses and organizations that collect personal electronic information.[116] The Decision takes a comprehensive approach to personal information and defines personal electronic information as "electronic information capable of identifying an individual or affecting personal privacy."[117] The Decision also requires organizations to publish policies regarding their data collection practices.[118] They must inform individuals of the purpose, method, and scope of data

---

[112] Mette Huss, *The Commercial Use of Open Source Software*, Newsletters: Technology Newsletter 03/2013, HANNES SNELLMAN, http://www.hannessnellman.se/news-seminars/newsletters/technology-newsletter-032013 (last visited June 30, 2014).

[113] Monika Kuschewsky, *European Council Taps the Breaks--Adoption of EU General Data Protection Regulation Delayed*, INSIDE PRIVACY (Oct. 28, 2013), http://www.insideprivacy.com/international/european-union/council-steps-on-the-brake---adoption-of-eu-general-data-protection-regulation-delayed/.

[114] The Hogan Lovells Privacy Team, *Making Sense of China's New Privacy Laws*, PRIVACY TRACKER (June 28, 2013), https://www.privacyassociation.org/privacy_tracker/post/making_sense_of_chinas_new_privacy_laws.

[115] *Id.*

[116] Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Jiaqiang Wangluo Xinxi Baohu de Jueding [National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 28, 2012, effective Dec. 28, 2012), http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm (China), English translation *available at* http://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/.

[117] The Hogan Lovells Privacy Team, *supra* note 114.

[118] *Id.*

collection.[119] Additionally, organizations must obtain an individual's consent prior to collecting any personal electronic information.[120]

The Decision also has several provisions aimed at protecting the individual's information after collection. The Decision requires organizations to implement measures to protect individuals' personal electronic information from theft and loss.[121] Data collectors are prohibited from selling or illegally disclosing personal electronic information (presumably without the user's consent), and must take immediate remedial measures if personal electronic information is compromised.[122] The Decision also cracks down on spam. Organizations must refrain from sending commercial electronic communications to a recipient's landline, mobile phone, or email address without consent.[123]

In April of 2013, the People's Congress also released draft amendments to the country's twenty-year-old consumer protection laws.[124] The proposed draft would amend nearly half of the current laws to address e-commerce issues.[125] The amendments are in line with the Decision's provisions regarding notice, consent, and disclosure. The draft amendments would also contain provisions addressing electronic commercial communications (spam) and mandate security of personal information held by data collectors.[126] The updated consumer protection law would even grant certain associations the right to file suit against companies allegedly infringing the rights of large groups of consumers.[127] Legal liabilities are divided between civil liabilities and administrative liabilities.

Civil liabilities are available when businesses infringe consumers' rights regarding their "names, images, privacy or other rights involving personal information."[128] Businesses will be ordered to "cease the infringement, restore

---

[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] Zhonghua Renmin Gongheguo Xiaofeizhe Quanyi Baohu Fa [Law on the Protection of Consumer Rights and Interests] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 25, 2013, effective Mar. 15, 2014), http://www.gov.cn/flfg/2013-10/25/content_2516547.htm (China); *see* Henry L.T. Chen, Jared Nelson & Samon Sun, *China Aims to Strengthen the Protection of Consumers' Personal Information*, LEXOLOGY (June 6, 2013), http://www.lexology.com/library/detail.aspx?g=a9fc2d17-1cf3-4621-a0a7-0f31bffbc1f8; *Amendments to Consumer Protection Law Allows for Public Interest Lawsuits with Limitations*, CONGRESSIONAL EXECUTIVE COMMISSION ON CHINA (Jan. 14, 2014), http://www.cecc.gov/publications/commission-analysis/amendments-to-consumer-protection-law-allows-for-public-interest#_edn3.
[125] The Hogan Lovells Privacy Team, *supra* note 114.
[126] *Id.*
[127] *Id.*
[128] Chen, Nelson & Sun, *supra* note 124.

any damages to the consumers' reputation, eliminate the bad effects of the violation, make apologies and compensate the victims."[129] Administrative penalties can also be severe. Businesses may be subject to "a warning, confiscation of unlawful earnings, the imposition of a fine up to RMB 500,000 or up to 10 times the value of the unlawful earnings, or may even have their business [license] suspended or revoked."[130]

Also in April 2013, China's Ministry of Industry and Information Technology (MIIT) issued a regulation governing smart devices.[131] The regulation prohibits smart phone manufacturers from "pre-installing" apps that "collect or modify users' personal information without their consent."[132] The regulation, effective November 1, 2013, also prohibits smart devices from "access[ing] networks without expressly notifying users and obtaining their consent," or "infring[ing] on the safety or security of users' personal information."[133] Device manufacturers must already obtain network access licenses for all devices they manufacturer, and this new regulation will require manufacturers to disclose information about the configuration of pre-installed apps to ensure compliance prior to licensing.[134]

The MIIT also issued non-binding guidelines in February 2013 for organizations that collect, use, and disclose personal information through information systems.[135] While these do not have the force of law, they will likely serve as a useful reference in enforcement actions or litigation.[136] These guidelines include many of the same provisions as the Decision on Strengthening Protection of Online Information. Data collecting organizations must notify individuals of the purpose and scope prior to collection, obtain consent prior to collection, and process the collected information consistent with such notice.[137] Additionally, data collectors must obtain express consent for the

---

[129] *Id.*

[130] *Id.* RMB 500,000 is the equivalent of about $82,000.

[131] Guanyu Jiaqiang Yidong Zhineng Zhongduan Guanli de Tongzhi [Notice Regarding Strengthening the Management of Network Access for Mobile Smart Terminals] (promulgated by the Ministry of Industry and Information Technology, Apr. 19, 2013, effective Nov. 1, 2013), http://dgj.miit.gov.cn/n11293472/n11295276/n11297773/15350110.html (China); *see* Scott Livingston, *China Regulates Smart Device Manufacturers' Use of Pre-installed Apps*, INSIDE PRIVACY (May 2, 2013), http://www.insideprivacy.com/emerging-technologies/china-regulates-smart-device-manufacturers-use-of-pre-installed-apps-1/; The Hogan Lovells Privacy Team, *supra* note 114.

[132] The Hogan Lovells Privacy Team, *supra* note 114.

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

processing of sensitive data and for cross-border transfers of any personal information.[138]

China's efforts to protect Internet privacy can provide useful guidance for our legislature as it attempts to craft legislation. However, the Chinese initiatives are far from complete. MIIT's guidelines do not provide a definition of "sensitive data," and the Decision does not detail how individual consent must be obtained or the types of remedial measures that should be taken in the event personal information is compromised.[139] MIIT's smart device regulations only regulate pre-installed apps and do not regulate apps downloaded after purchase.[140] Perhaps future legislation will address third-party and post-purchase installed apps.

Most importantly, before we laud the People's Republic's attempt at Internet privacy, it should also be noted that the MIIT's regulations also prohibit smart device manufacturers from pre-installing apps that "contain content restricted by Chinese law; e.g., obscenity and anti-government speech."[141] In the United States the federal government might lawfully be able to regulate obscenity, but it most certainly cannot prohibit anti-governmental speech due to First Amendment protections.[142] Congress would be wise to study the effectiveness of each part of the Chinese laws and incorporate the most effective pieces into domestic legislation.

III. DOMESTIC STRATEGIES TO PROTECT ONLINE PRIVACY

Both Congress and several states have proposed legislation aimed at addressing Internet privacy concerns. While the proposals are numerous, the number of proposals that become law is minimal. It seems every few months a re-hashed version of a previous bill is thrown into the Congressional hopper. Highlighted below are a few innovative federal bills, as well as California's attempt to pick up the slack where the Feds have failed to act.

A. Federal Legislation

1. Mobile Device Privacy Act - H.R. 6377 (112th)

Senator (and former Representative) Edward Markey from Massachusetts has proposed several bills relating to online privacy. In 2012, Markey proposed the Mobile Device Privacy Act while still a member of the House of

---

[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *See, e.g.*, Hess v. Indiana, 414 U.S. 105 (1973); Paris Adult Theatre I v. Slaton, 413 U.S. 49 (1973); Brandenburg v. Ohio, 395 U.S. 444 (1969).

Representatives.[143] This Act is aimed at data collection by smartphone apps and the subsequent transfer of the collected data. The Act would push for many of the same protections provided by China's regulations governing smart devices.[144] The Act would require sellers and manufacturers of mobile devices and software to disclose the capability of any installed software to monitor mobile device usage.[145] The consumer must be told that the monitoring software is installed, what it is monitoring, with whom that information might be shared, and how the information will be used.[146] The Act would require the express consent of a consumer before the monitoring software begins collecting and transmitting any information.[147] The Act defines "monitoring software" as software with the "capability to monitor the usage of a mobile device or the location of the user and to transmit the information collected to another device or system, whether or not such capability is the primary function of the software or the purpose for which the software is marketed."[148]

In public statements, Markey recognized that "[a]pps very commonly access our sensitive information . . . without prior notice and even when the app isn't actively being used."[149] In addition to making companies disclose and obtain permission before monitoring a mobile device, Markey's bill would require any company that collects personal information from a mobile device to have secure policies in place for storing it.[150] The bill does not detail what these policies are, but calls for standards to be set, and met, to protect collected information.[151]

The bill would give enforcement powers to the Federal Trade Commission and the Federal Communications Commission (FCC) to punish mobile companies that break the law and provide a clear-cut way for customers to sue companies that violated their privacy. A violation would either be treated as a violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act[152] or a violation of the Communications Act of 1934.[153] The

---

[143] Mobile Device Privacy Act, H.R. 6377, 112th Cong. (2nd Sess. 2012).

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

[145] H.R. 6377.

[146] Alex Wilhelm, *Meet the Mobile Device Privacy Act: A New Bill to Protect Mobile Consumers that Is Already Causing a Stir*, THE NEXT WEB (Sept. 13, 2012, 2:06 AM), http://thenextweb.com/us/2012/09/13/meet-mobile-device-privacy-act-a-strict-new-bill-protect-mobile-consumers-already-causing-stir/.

[147] H.R. 6377.

[148] *Id.*

[149] Weitzenkorn, *supra* note 39.

[150] Grant Gross, *Lawmaker Pushes Mobile Privacy Legislation*, PCWORLD (Sept. 12, 2012, 11:30 AM), http://www.pcworld.com/article/262244/lawmaker_pushes_mobile_privacy_legislation.html.

[151] Wilhelm, *supra* note 146.

[152] 15 U.S.C. § 57a(a)(1)(B) (2012).

[153] 47 U.S.C. § 151–614 (2006).

Act would authorize civil enforcement actions by states and by private persons injured by an act in violation of such regulations.[154] An unintentional infraction would be worth up to $1,000 in damages per violation, and "willful" or "knowing" violations call for damages triple that of an unintentional violation.[155]

The Act also contains an opt-out provision requiring that the consumer be granted the opportunity to prohibit data collection and transmission at any time.[156] Opting out of these tracking regimes is a crucial tool for consumers who are sensitive about their data being collected and/or shared. While the Mobile Device Privacy Act appears to have died,[157] several other pieces of legislation have been proposed in recent years relating to an "opt-out" or "Do-Not-Track" option for consumers.

2. Do Not Track Online Act of 2013 (113th)

Do-Not-Track has become a popular piece of legislation over the past few years. Since 2011, several iterations of Do-Not-Track legislation have been introduced in the House and Senate including, the "Do Not Track Me Online Act"[158] by Representative Jackie Speier, the "Consumer Privacy Protection Act of 2011"[159] by Representatives Stearns and Matheson, and the "Commercial Privacy Bill of Rights Act of 2011"[160] proposed by Senators Kerry and McCain. All these bills carry the same goal: provide consumers an enforceable tool to express their preference not to be tracked.[161]

Most recently, Senators John D. (Jay) Rockefeller IV and Richard Blumenthal introduced the Do-Not-Track Online Act of 2013.[162] This bill provides consumers a legally-enforceable mechanism to express their preference

---

[154] Mobile Device Privacy Act, H.R. 6377, 112th Cong. (2nd Sess. 2012).

[155] *Id.*

[156] *Id.*

[157] *H.R. 6377 (112th): Mobile Device Privacy Act*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/hr6377#overview (last visited June 16, 2014).

[158] Do Not Track Me Online Act, H.R. 654, 112th Cong. (1st Sess. 2011).

[159] Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (1st Sess. 2011).

[160] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (1st Sess. 2011).

[161] *See* Joshua A.T. Fairfield, *Do-Not-Track as Default*, 11 NW. J. TECH. & INTELL. PROP. 575, 582 (2013).

[162] Do-Not-Track Online Act of 2013, S. 418, 113th Cong. (2013); *see S. 418 (113th): Do-Not-Track Online Act of 2013*, GOVTRACK.US, https://www.govtrack.us/congress/bills/113/s418#overview (last visited June. 16, 2014).

to not be tracked online.[163] Once a consumer expresses his or her preference to not be tracked, companies must honor these requests. The bill permits the Federal Trade Commission to pursue enforcement actions against any company that does not honor these requests by consumers.[164] The bill still allows companies to collect information that is necessary for the website or online service to function and be effective.[165] However, the online companies then have a legal obligation "to destroy or anonymize the information once it is no longer needed."[166]

The technology behind Do-Not-Track is quite simple. "Every time your computer sends or receives information over the Web, the request begins with some short pieces of information called headers."[167] These headers include information like which browser you are using, your computer's language setting, and other technical details.[168] "The Do-Not-Track proposal is to include a simple, machine-readable header indicating that you don't want to be tracked."[169] The Do-Not-Track header would read: DNT:1.[170]

The Electronic Frontier Foundation provides a simple definition of tracking: "the retention of information that can be used to connect records of a person's actions or reading habits across space, cyberspace, or time."[171] The Do-Not-Track header prevents this. Also significant is that there is no "list" that consumers need to sign up for.[172] Early discussion of Do-Not-Track included having a list-based registry of users, similar to the Do Not Call Registry, but the current proposal does not incorporate a central list of consumer data.[173]

---

[163] Press Release, U.S. Senate Committee on Commerce, Science, and Transportation, Rockefeller Introduces Do-Not-Track Bill to Protect Consumers Online (Feb. 28, 2013) http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=daf20f21-be4a-4b84-bbb1-e271730a8813&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=505cc3fa-a767-40f4-8ac2-4b8326b44e94&MonthDisplay=2&YearDisplay=2013.

[164] *Id.*

[165] Katy Bachman, *Rockefeller Reintroduces Do Not Track Act: Privacy Heats Up Again in Congress*, ADWEEK (Feb. 28, 2013, 5:46 PM), http://www.adweek.com/news/technology/rockefeller-reintroduces-do-not-track-act-147610.

[166] *Id.*

[167] *Do Not Track – The Technology*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/do-not-track (last visited June 16, 2014).

[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] *What Does the "Track" in "Do Not Track" Mean?*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean (last visited June 16, 2014).

[172] *Do Not Track – The Technology*, *supra* note 167167.

[173] *Id.*

Most browsers, including Google Chrome, Mozilla Firefox, and Apple's Safari, already possess a Do-Not-Track feature that users can activate in their browser settings. Microsoft's Internet Explorer 10 is the first browser to make Do-Not-Track the default setting.[174] Recently, Apple added a feature to the iPhone to allow users to activate the Do-Not-Track setting in mobile Safari for iOS 7.[175] However, this feature only affects Safari, is unlikely to have any effect on tracking conducted by third-party apps, and users must take additional steps to disable location-based tracking such as location-based iAds.[176] Bob Liodice, the President and Chief Executive Officer of the Association of National Advertisers, argues that "[c]ompanies are increasingly offering consumers new privacy features and tools such as sophisticated preference managers, persistent opt outs, universal choice mechanisms, and shortened data retention policies."[177] Liodice believes that these "developments demonstrate that companies are responsive to consumers and that companies are focusing on privacy as a means to distinguish themselves in the marketplace."[178]

The problem that remains is that webhosts and advertisers are free to ignore this setting because it is not legally binding in any way. A few companies have chosen to voluntarily recognize a user's Do-Not-Track request, but many advertisers simply ignore it.[179] Additionally, even if advertisers honor the header, users will likely see the same number of ads; the ads just will not be specifically targeted towards particular users based on their browsing history. In fact, when one activates Do-Not-Track on Google Chrome, that user receives the following warning:

> Enabling 'Do Not Track' means that a request will be included with your browsing traffic. Any effect depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example to improve security, to provide content,

---

[174] Drew Bowling, *Internet Explorer 10 First Browser with 'Do Not Track' by Default*, WEBPRONEWS (June 1, 2012), http://www.webpronews.com/internet-explorer-10-first-browser-with-do-not-track-by-default-2012-06.

[175] Aaron Souppouris, *The Best Hidden Features in iOS 7*, THE VERGE (Sept. 18, 2013, 1:31 PM), http://www.theverge.com/2013/9/18/4741412/the-best-hidden-features-in-ios-7.

[176] Jason D. O'Grady, *Four Privacy Settings You Should Enable in iOS 7 Immediately*, ZDNET (Sept. 19, 2013, 7:37 AM), http://www.zdnet.com/four-privacy-settings-you-should-enable-in-ios-7-immediately-7000020902/.

[177] Fairfield, *supra* note 161161, at 619 n.245.

[178] *Id.*

[179] *See* Ed Bott, *Why Do Not Track Is Worse than a Miserable Failure*, ZDNET (Sept. 21, 2012, 5:35 AM), http://www.zdnet.com/why-do-not-track-is-worse-than-a-miserable-failure-7000004634/.

> services, ads and recommendations on their websites, and to generate reporting statistics.

This warning summarizes nicely how little Do-Not-Track does without recognition by tracking companies.

In recent months it appears the effort to establish a voluntary Do-Not-Track solution has "died."[180] As of September 2013, the Digital Advertising Alliance has formally pulled out of the 110-member Tracking Protection Working Group (TPWG).[181] The TPWG had been engaged in a "futile" two-and-a-half-year-old process to establish a universal Do-Not-Track standard.[182] This is perhaps evidence to support Senator Rockefeller's belief that "the online advertising industry has no incentive to provide consumers with strong privacy protections," and that "[l]egislation is the only way to give consumers more control over their personal information."[183]

With the voluntary effort to standardize Do-Not-Track regulations failing, the Do-Not-Track Online Act of 2013 is perhaps one way to force advertisers and data collection companies to respect consumers' wishes to not be tracked. The bill was referred to committee shortly after introduction in February.[184] It remains unclear whether Congress will actually pass any legislation aimed at protecting consumers' Internet privacy.

3. Do Not Track Kids Act of 2013 (113th)

Now in the United States Senate, Senator Markey has continued proposing legislation aimed at Internet privacy. On November 14, 2013, Markey, co-sponsored by Republican Representative Joe Barton, proposed the Do Not Track Kids Act of 2013.[185] The Do Not Track Kids Act expands the privacy protections of the Children's Online Privacy Protection Act of 1998 (COPPA)[186] and allows parents and teens more control over what information is collected about them and how that information is used.[187] The bill provides many of the same protections that the Do Not Track Online Act of 2013

---

[180] Stephen Shankland, *Advertiser Group: Do Not Track Web Privacy Effort Is Dead*, CNET (Sept. 18, 2013, 9:01 AM), http://news.cnet.com/8301-1023_3-57603473-93/advertiser-group-do-not-track-web-privacy-effort-is-dead/.

[181] Katy Bachman, *Digital Advertising Alliance Exits Do Not Track Group Development Could Renew Calls for Privacy Laws*, ADWEEK (Sept. 17, 2013, 12:40 AM), http://www.adweek.com/news/technology/digital-advertising-alliance-exits-do-not-track-group-152475.

[182] *Id.*

[183] *Id.*

[184] Do-Not-Track Online Act of 2013, S. 418, 113th Cong. (2013).

[185] Do Not Track Kids Act of 2013, S. 1700, 113th Cong. (2013).

[186] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012).

[187] Herb Weisbaum, *Bill Would Limit Online Tracking, Give Teens 'Eraser Button'*, CNBC (Nov. 18, 2013, 6:00 AM), http://www.cnbc.com/id/101202798.

contains, but applies them only to individuals fifteen and younger. The bill also creates an "eraser button" that allows teens and parents to delete publicly-available personal information when it is "technologically feasible."[188]

Under COPPA, websites are required to obtain written parental permission before a website can collect, use, or disclose personal information about kids twelve and younger.[189] The Do Not Track Kids Act establishes a "Digital Marketing Bill of Rights for Teens" that expands this protection to anyone under the age of thirteen. It would also prohibit Internet companies from collecting personal and location information from anyone between thirteen and fifteen years old without the user's consent.[190]

The bill requires informed consent. Internet companies must explain the types of personal information collected, and how that information is used and disclosed.[191] The disclosure must explicitly detail the company's policies for collection of personal information.[192] The bill also cracks down on targeted advertising towards teens under the age of fifteen by requiring consent from the parent or teen before targeted advertising can be sent to that teen.[193]

Consumer groups, including Consumer Action and Consumer Watchdog, believe self-regulation has failed and that Congress should step in to address some of the marketing practices that have "started to cross the line."[194] These groups support the type of legislation that would "limit the ability of marketers to track children online, especially their location, and use this information to deliver targeted marketing."[195]

Giving kids the opportunity to opt out of online tracking is perhaps less objectionable and creates a lesser burden than implementing a national opt-out system. Children and teens are perhaps more vulnerable to online tracking and advertising. Jim Steyer, Common Sense Media's CEO, recognized that "[t]oday's kids are living so much of their lives online and are forfeiting their right to privacy before they fully understand what privacy is."[196] Steyer believes that "kids and families should have the right to control their privacy and personal information online."[197]

---

[188] Andrew Couts, *Facebook Won't Like This New Teenager Privacy Bill*, DIGITAL TRENDS (Nov. 15, 2013), http://www.digitaltrends.com/social-media/facebook-do-not-track-kids-act/. For a detailed discussion on "Eraser" laws, see *infra* Part III.B.1.

[189] Couts, *supra* note 188.

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] Weisbaum, *supra* note 187187.

[195] *Id.*

[196] Jim Steyer, *Do Not Track Kids Act of 2013 Introduced in Congress*, HUFFINGTON POST (Nov. 15, 2013, 12:36 PM), http://www.huffingtonpost.com/common-sense-media/do-not-track-kids-act-of-_b_4277005.html.

[197] *Id.*

This legislation comes at a time when Facebook has relaxed privacy rules such that children aged thirteen to seventeen now have the option to share photos, updates, and comments with the general public on Facebook.[198] Teens can also activate the "follow" feature which "would allow anyone they're not friends with to see their public posts in the main news feed."[199] Senator Markey argues that the "speed with which Facebook is pushing teens to share their sensitive, personal information widely and publicly online must spur Congress to act commensurately to put strong privacy protections on the books for teens and parents."[200]

Could this bill actually pass? Similar legislation has already failed in 2011 and 2012.[201] However, Representative Barton believes with bipartisan support in both houses, "the third time could be the charm."[202]

B. State Legislation – California

California has taken it upon itself to pass legislation to protect online privacy for its citizens where the federal government has failed to act. California has already passed expansive protections for minors that use the Internet, which are scheduled to go into effect in 2015. California is also considering legislation to increase citizens' right to access information stored about them and increase transparency for California consumers in the digital age.

1. SB 568 - Privacy Rights for California Minors in the Digital World - The Minor "Eraser" Law

Senate Bill 568 has two main provisions that will be incorporated into California Business and Professions Code Sections 22580–22582.[203] Section 22580 aims to protect children and teens under the age of eighteen from targeted advertising of certain prohibited products.[204] This section prohibits operators of Internet websites, online services, online applications, and mobile apps from *knowingly* marketing and advertising a broad range of products to a minor.[205]

---

[198] Heather Kelly, *Facebook Changes Privacy Settings for Teens*, CNN (Oct. 31, 2013, 7:32 PM), http://www.cnn.com/2013/10/16/tech/social-media/facebook-teens-privacy/.

[199] *Id.*

[200] Couts, *supra* note 188.

[201] Weisbaum, *supra* note 187.

[202] *Id.*

[203] Privacy: Internet: minors, S.B. 568, 2013 stat. ch. 336, 2013-2014 Leg., Reg. Sess. (Cal. 2013) (to be codified at Cal. Bus. & Prof. §§ 22580–82), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

[204] *Id.*

[205] Lisa B. Kim & Joshua B. Marker, *Reference Guide to SB 568 - Internet Privacy for California Minors*, LEXOLOGY (Oct. 30 2013), http://www.lexology.com/library/detail.aspx?g=51f41457-8131-4da5-a22c-0f34ed681ed5 (emphasis added).

These prohibited products include: alcoholic beverages, firearms, ammunition, spray paint, tobacco products, fireworks, tanning services, dietary supplements, lottery tickets, tattoos, drug paraphernalia, and obscene material.[206] The prohibitions only apply to websites that are either "directed to minors" or that have actual knowledge that a minor is using the website.[207]

After the bill's passage in the Assembly in June, the Center for Democracy and Technology (CDT) argued that the bill was "unconstitutionally vague" as to what sites may be considered "directed to minors."[208] The CDT argued that this could leave website operators "with no certainty of their obligations under the law."[209] The assembly amended the bill to clarify that the bill's requirements will only apply to websites that are "predominantly" directed to minors.[210] The Senate then concurred in this amendment, and approved the amended bill unanimously.[211] This amendment was presumably sufficient to dissolve any ambiguity in the legislature's eyes because Governor Brown signed the bill into law on September 23, 2013.[212]

The bill also creates an "eraser button" that allows teens and parents to delete publicly-available personal information when it is "technologically feasible."[213] Section 22581 requires operators to notify minors of their rights to remove content or information they posted to the operator's website, online service, online application, and mobile app.[214] Operators will be required to honor requests to remove such data, subject to specified conditions and exceptions.[215]

As discussed in Part III.A.3 above, Facebook's relaxed privacy rules relating to teens will likely exacerbate the problem of "over-sharing" on the Internet. Commentators find this problem especially common with kids who "may not realize the potential consequences of disclosing personal information on social networks."[216] Notwithstanding its flaws, the eraser button could potentially provide a tool for teens and families to control their privacy and personal information online.[217]

---

[206] *Id.*
[207] *Id.*
[208] Paul Martino, *Inside Calif.'s New Online Privacy Law for Minors*, LAW360 (Oct. 11, 2013, 2:10 PM), http://www.law360.com/articles/479853/inside-calif-s-new-online-privacy-law-for-minors.
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *See id.*
[213] Couts, *supra* note 188.
[214] Kim & Marker, *supra* note 205.
[215] *Id.*
[216] Weisbaum, *supra* note 187.
[217] *See* Steyer, *supra* note 196.

A recent research poll performed by the Pew Research Center suggests that teens are already taking steps to manage their online reputations. The Pew poll found that fifty-nine percent of teens have deleted or edited something that they posted online in the past, and nineteen percent have posted updates, comments, photos, or videos that they "later regretted sharing."[218] Additionally, this eraser-type legislation is quite popular. A Common Sense Media poll found that ninety-four percent of adults and ninety-two percent of teens felt they should be able to request the deletion of all their personal information held by a search engine, social network, or marketing company after a specific time period.[219] It remains uncertain whether it is actually possible to truly delete "all" personal information.

Critics of the "eraser button" argue the legislation is unlikely to have any effect on privacy. Gregory Ferenstein of *TechCrunch* argues this type of legislation is duplicative because "nearly every imaginable service [already] offers a delete button."[220] More importantly, it fails to recognize that "few posts exist in isolation."[221] It is nearly impossible to delete information from the Internet because "embarrassing photos spread virally, and Internet archives automatically create copies of nearly every piece of information on the web."[222] To have real bite, the measure would need to address content that has been reposted, archived, or interacted with through likes, comments, and retweets.[223]

However, now that "Facebook likes" are constitutionally-protected speech, removing these third-party posts may place personal privacy at odds with the First Amendment.[224] Additionally, Ferenstein argues that this "comes dangerously close to the European Union's proposed 'right to be forgotten.'"[225] Jeffrey Rosen, a law professor at George Washington University, explained that the "right to be forgotten could make Facebook and Google . . . liable for up to two percent of their global income if they fail to remove photos that people post

---

[218] Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, & Meredith Beaton, *Teens, Social Media, and Privacy*, PEW RESEARCH CENTER (May 21, 2013), http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy/Summary-of-Findings.aspx.

[219] Jim Steyer, *Why Kids Need an "Eraser Button"*, COMMON SENSE MEDIA (Sept. 19, 2013), http://www.commonsensemedia.org/blog/why-kids-need-an-eraser-button.

[220] Gregory Ferenstein, *On California's Bizarre Internet Eraser Law for Teenagers*, TECHCRUNCH (Sept. 24, 2013), http://techcrunch.com/2013/09/24/on-californias-bizarre-internet-eraser-law-for-teenagers/.

[221] Katy Waldman, *California's Internet Eraser Law: Nice Idea, but It Won't Work*, SLATE (Sept. 25, 2013, 3:07 PM), http://www.slate.com/blogs/xx_factor/2013/09/25/sb_568_california_digital_eraser_law_for_minors_is_unlikely_to_work.html.

[222] Ferenstein, *supra* note 220.

[223] Waldman, *supra* note 221.

[224] *See* Bland v. Roberts, 730 F.3d 368, 386 (4th Cir. 2013).

[225] Ferenstein, *supra* note 220.

about themselves and later regret, even if the photos have been widely distributed already."[226] This simple "easer button" legislation would result in "a whole new body of case law dedicated to choosing when the right to be forgotten trumps our right to share and discuss information."[227] As Ferenstein put it: "From here, things are only going to get more bizarre."[228]

2. The Right to Know Act (AB 1291)

California is also taking steps to give consumers the right to see what information tracking companies are collecting and sharing about them. The Right to Know Act (AB 1291) updates California's outdated transparency laws and attempts to place some power in the hands of consumers.[229] The central focus of the Right to Know Act is transparency, or the "right of access" as defined in the European Union Directive. The Act grants California consumers the opportunity to request, and requires a company to give users access to, the personal data the company has collected on them, and a list of any other companies with whom they have shared the user's personal data.[230] The Act would cover California residents and would apply to both offline and online companies.[231] The law is only about transparency, and does not create any new restrictions on data sharing.[232]

Under current California law, customers can contact companies and ask for an accounting of disclosures made by companies for direct marketing purposes only.[233] The new proposal allows California consumers to request an accounting of "all the ways their personal information is being trafficked."[234] This expands current law to include online advertisers, data brokers, and third-party apps.[235] This ensures that users can track the flow of their data from online

---

[226] *Id.*
[227] *Id.*
[228] *Id.*
[229] Privacy: Right to Know Act of 2013, A.B. 1291, 2013-2014 Leg., Reg. Sess. (Cal. 2013), *available at* http://leginfo.ca.gov/pub/13-14/bill/asm/ab_1251-1300/ab_1291_bill_20130222_introduced.pdf.
[230] Rainey Reitman, *New California "Right to Know" Act Would Let Consumers Find Out Who Has Their Personal Data -- and Get a Copy of It*, ELECTRONIC FRONTIER FOUNDATION (Apr. 2, 2013), https://www.eff.org/deeplinks/2013/04/new-california-right-know-act-would-let-consumers-find-out-who-has-their-personal.
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *Id.*

interactions.[236] The Act also updates the definitions to include location data, which is not adequately protected by current law.[237]

The stated rationale behind the law is basic: California hopes to shed light into the "largely hidden, highly lucrative world of the personal data economy."[238] With insight into what information is collected, and with whom that information is shared, policy makers hope to fashion legislation in the future to regulate the personal data economy to better protect personal privacy.[239] The bill's sponsor, Bonnie Lowenthal, a Democratic assemblywoman from Long Beach, argues that telemarketing is no longer the biggest problem with privacy, and it is time for an update in state law to cover the "many different mobile apps that can track location and spending habits . . . ."[240]

The American Civil Liberties Union (ACLU) is currently battling the tech lobby for support of the bill. Tech America, which represents companies such as Google and Facebook, argues the bill "would open up businesses to an avalanche of requests from individuals as well as costly lawsuits."[241] Like most Internet legislation, it looks like the tech lobby has successfully stalled the bill, as Lowenthal decided to delay further action on the bill.[242]

IV. THE SOLUTION(S)?

Any legislation aimed at protecting Internet privacy should aim at shedding light on what information is being collected, and provide some enforceable mechanism for consumers to opt out of Internet tracking. A Do-Not-Track regime should grant consumers the opportunity to voice their opposition to being tracked, and require that the preference be honored. Thus far, any attempt for the market to establish voluntary compliance with Do-Not-Track headers has failed. Critics argue that advertisers have no incentive to provide robust privacy protections for consumers because they derive much of their

---

[236] *Id.*

[237] *Id.*

[238] *Id.*

[239] *See id.*

[240] Vauhini Vara & Geoffrey A. Fowler, *New Online-Data Bill Sets Up Privacy Fight*, WALL ST. J. (Apr. 5, 2013, 7:13 PM), http://online.wsj.com/news/articles/SB10001424127887323916304578402912554668102.

[241] Steven Harmon, *Silicon Valley Companies Quietly Try to Kill Internet Privacy Bill*, SAN JOSE MERCURY NEWS (Apr. 20, 2013, 12:00 PM), http://www.mercurynews.com/politics-government/ci_23067322/silicon-valley-companies-quietly-try-kill-internet-privacy.

[242] Press Release, Assemblymember Bonnie Lowenthal, California State Assembly District 70, Right to Know Act Stalled for the Year (May 2, 2013) http://asmdc.org/members/a70/news-room/press-releases/right-to-know-act-stalled-for-the-year; *see* Harmon, *supra* note 241.

revenue from Internet tracking and profiling.[243] I disagree. The incentives have simply not been sufficient so far. People are still using Google even though they (should) know that their online activity is being tracked. Presumably it does not bother a significant number of consumers enough to stop or switch services. If companies are not losing visitors due to their tracking policies, why change?

One solution is to implement a legally-binding Do-Not-Track regime. As outlined above, the technology is simple. Users may simply activate the Do-Not-Track preference in their browser or mobile device. This preference, however, must be universally applicable to cookies, mobile apps, in-store mobile analytics software, and traditional web browsing. It should also be simple, with clear instructions provided by the software or device provider. A legally-binding Do-Not-Track regime would only require a law mandating that webhosts (or controllers) honor the users' preference. There does not need to be, nor should there be, a centralized Do-Not-Track list. A government-controlled centralized list carries privacy risks of its own.[244]

The legislation should permit the FTC or FCC to impose fines or other administrative sanctions similar to those in China's draft amendments discussed above.[245] In addition, the legislation should also provide individuals with a legal claim against companies who do not honor their preference to not be tracked. However, administrative enforcement is likely to be more successful as many individuals will lack the time and resources to litigate against information-collecting giants such as Google.

Some argue the system should be Do-Not-Track by default, thus requiring individuals to opt in if they do not mind being tracked.[246] This, however, is not necessary and poses greater consequences than an opt-out system. Any opt-out regime runs the risk of fundamentally altering the economic paradigm of the Internet. If enough people opt out, service providers will be stripped of the economic incentive to offer free services. Without advertising revenue, it is unlikely that Google will continue to offer free services such as Gmail, Google Drive, and Google Docs. If everyone is automatically opted out, it is likely far fewer people would opt in, thus exacerbating this problem.[247] A Do-Not-Track by default system might even cause behavioral advertising to "wither to insignificance," even though it offers value for many customers, "most of whom don't mind the practice."[248]

---

[243] *See* Bachman, *supra* note 181 (quoting Sen. Jay Rockefeller).

[244] For a look at the privacy implications of a centralized list, see Joshua A.T. Fairfield, *Cracks in the Foundation: The New Internet Legislation's Hidden Threat to Privacy and Commerce*, 36 ARIZ. ST. L.J. 1193, 1205–16 (2004).

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

[246] *See* Fairfield, *supra* note 161, at 575.

[247] *See id*. at 616.

[248] Curt Hessler, The Wars of Digital Prosperity 61–64 (2013) (unpublished manuscript) (on file with author).

Additionally, the Digital Advertising Alliance (DAA) argues against Do-Not-Track as the default setting because it purportedly does not represent user choice.[249] The DAA even declared it would ignore Internet Explorer's Do-Not-Track header because Microsoft (by way of Internet Explorer 10) was essentially making the Do-Not-Track decision on behalf of its users.[250] An opt-out regime would likely suffice so long as it permits privacy-concerned individuals to browse anonymously at their election, and the DAA would have no argument against the choice manually activated by the user.

Enforcement legislation might not be the best solution to the problem. Critics, including Michigan Congressman Fred Upton, are highly skeptical of Congress' or the government's ability to "keep up with the innovative and vibrant pace of the Internet without breaking it."[251] Upton believes that "[c]onsumers and the economy as a whole will not be well served by government attempts to wrap the Web in red tape."[252] As detailed above, the E.U. Directive has already been criticized for failing to keep up with innovation as the rules on data exportation and transfer to third countries were deemed "outmoded" by the RAND Corporation.[253] This is perhaps a compelling argument considering the government's inability to build a functioning health care website after throwing $600 million at it.[254]

Enforcement legislation also fails to address the global nature of the Internet. As seen with the E.U. Directive, enforcement outside the sovereign's jurisdiction is impossible without international cooperation, thus inhibiting the effectiveness of the privacy program. The world, along with the Internet, will only become increasingly more globalized. Considering the United States has yet to institute an opt-out protocol on a national scale, it is very unlikely a global consensus will be reached to establish an international standardized opt-out protocol. The free market, however, can traverse international borders.

Enforcement legislation may not be required if the market can incentivize companies to honor Do-Not-Track requests by users or alter their profiling practices to dissuade consumer discomfort. Transparency or "right of access"

---

[249] Katy Bachman, *Take That, Microsoft: Digital Ad Community's Final Word on Default Do Not Track*, ADWEEK (Oct. 9, 2012, 10:17 AM), http://www.adweek.com/news/technology/take-microsoft-digital-ad-communitys-final-word-default-do-not-track-144322.

[250] *Id.*; *see supra* Part III.A.2.

[251] Grant Gross, *Could New Online Privacy Laws Lead to Unnecessary Regulation?*, PCWORLD (Mar. 29, 2012 2:59 PM), http://www.pcworld.com/article/252865/critics_say_ftc_obama_privacy_plans_would_lead_to_major_regulation.html.

[252] *Id.*

[253] *See supra* Part II.A.1.

[254] Brett Norman & Jason Millman, *Doubts About Healthcare.Gov Repair Date*, POLITICO (Nov. 13, 2013, 5:10 PM), http://www.politico.com/story/2013/11/darrell-issa-obamacare-hearing-99788.html.

laws (as seen in the E.U. Directive and PRC Decision) could provide this incentive. If users are permitted access to what information is collected about them, and how that information is used, perhaps we can indeed shed light on the largely hidden, highly lucrative world of the personal data market. If users object to the type of information collected or the way in which the information is used, consumers can opt out. If the opt-out preference is not honored, consumers can voice their opinions in other ways. Users can essentially "vote with their feet" by switching to services that have less intrusive tracking policies or to companies that honor tracking requests. When companies begin to experience a loss in revenue by way of fewer active users, they will be forced to alter their practices. Twitter has recently announced it will honor Do-Not-Track settings in users' browsers when it launches its ad exchange.[255] Perhaps this is evidence that the market is gradually adapting to consumer preference in this area.

Google and other "free" service providers could incentivize individuals to forego opting out in exchange for access to these free services. Additionally, Google could offer these same services for a fee to consumers who choose to opt out of tracking. This would place a value on an individual's privacy on the Internet. If users place a value on their Internet privacy that is higher than the fee charged for these services, they will continue to opt out. However, if users wish to continue to use the free services, they can do so in exchange for their consent to tracking by the service provider. Essentially, this places a monetary value on a user's browsing profile and can at least provide some return to the users whose data is being collected and exploited. It is perhaps a utopian idea of market economics, and it is unclear whether such a system would be sustainable, but it is an alternative solution to a stagnant legislature who has failed to seriously address online privacy.

CONCLUSION

While much has been thrown into the Congressional hopper to combat online tracking, nothing has appeared to stick. Little has passed, and even less has been effective. This Note examined the different approaches taken in the United States and abroad and analyzed the potential effectiveness of each proposal. It is in our country's best interest for Congress to incorporate the effective parts of each approach into a simple Internet privacy regime. A Do-Not-Track regime must grant consumers the opportunity to voice their opposition to tracking, and through legislation or private contract, require that their preferences be honored. While Congress procrastinates, efforts should be focused on developing a voluntary Do-Not-Track system in the private sector that emphasizes transparency and informed user consent.

---

[255] Jim Edwards, *Twitter May Have Handed Microsoft a Huge Victory in Its War Against Google*, BUSINESS INSIDER (July 5, 2013, 12:34 PM), http://www.businessinsider.com/twitter-microsoft-and-google-and-do-not-track-2013-7.