To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising

Omer Tene[1] and Jules Polonetsky[2]

Table of Contents

[1] Associate Professor, College of Management Haim Striks School of Law, Israel; Affiliate Scholar, Stanford Center for Internet and Society; Fellow, Center for Democracy and Technology. I would like to thank the College of Management Haim Striks School of Law research fund and the College of Management Academic Studies research grant for supporting research for this article.
[2] Co-chair and Director, Future of Privacy Forum. The authors would like to thank Christopher Wolf, Michael Birnhack, Boris Segalis and the participants at the Privacy Law Scholars Conference in Berkeley for their helpful comments.

Abstract

The past decade has seen a proliferation of online data collection, processing, analysis and storage capacities leading businesses to employ increasingly sophisticated technologies to track and profile individual users. The use of online behavioral tracking for advertising purposes has drawn criticism from journalists, privacy advocates and regulators. Indeed, the behavioral tracking industry is currently the focus of the online privacy debate. At the center of the discussion is the Federal Trade Commission's Do Not Track (DNT) proposal. The debate raging around DNT and the specific details of its implementation disguises a more fundamental disagreement among stakeholders about deeper societal values and norms. Unless policymakers address this underlying normative question – is online behavioral tracking a social good or an unnecessary evil – they may not be able to find a solution for implementing user choice in the context of online privacy. Practical progress advancing user privacy will be best served if policymakers and industry focus their debate on the desirable balance between efficiency and individual rights and if businesses implement tracking mechanisms fairly and responsibly. Policymakers must engage with these underlying normative questions; they cannot continue to sidestep these issues in the hope that "users will decide" for themselves.

1. Introduction

For many years, internet users considered online activity to be confidential, their whereabouts protected by a veil of anonymity. This approach was best captured by the famous New Yorker

cartoon-cum-adage "On the internet, nobody knows you're a dog".[3] The reality alas is quite different. The actions of most internet users, every search, query, click, page view and link, are logged, retained, analyzed and used by a host of third parties, including websites (also known as "publishers"), advertisers, and a multitude of advertising intermediaries, including ad networks, ad exchanges, analytics providers, re-targeters, market researchers, and more. Although users may expect that many of their online activities are anonymous, the architecture of the internet allows multiple parties to collect data and compile user profiles with various degrees of identifying information.[4]

The value created by online advertising, which fuels the majority of free content and services available online, has been immense. Online advertising is greatly enhanced by the ability to analyze and measure the effectiveness of ad campaigns and by online behavioral tracking, which involves tracking of users' online activities in order to deliver tailored ads. The more finely tailored the ad, the higher the conversion or "clickthrough" rate, and thus the revenues of advertisers, publishers, and ad intermediaries. In the past decade, the number and quality of online data collection technologies have increased. The collection and use of large amounts of data to create detailed personal profiles have clear privacy implications. Users have remained largely oblivious to the mechanics of the market for online information, including data collection processes, prospective data uses, and the identity of the myriad actors involved. While users clearly benefit from the rich diversity of content and services provided without charge, such benefits need to be weighed against the costs imposed on users' privacy.

The behavioral tracking industry is currently the focus of the online privacy debate. At the center of the discussion is the Federal Trade Commission's Do Not Track (DNT) proposal. We argue that this is because the simplicity of DNT crystallizes the deep ideological divide about right and wrong in online activities. The debate raging around DNT and the specific details of its implementation (opt-in; opt-out; browser, cookie or black list based; etc.) disguise a more fundamental disagreement among stakeholders about deeper societal values and norms. Unless policymakers address this underlying normative question – is online behavioral tracking a social good or an unnecessary evil – they may not be able to find a solution for implementing user choice in the context of online privacy. Practical progress advancing user privacy will be better served if policymakers and industry focus their debate on the desirable balance between efficiency and individual rights and if businesses implement tracking mechanisms fairly and responsibly.

By emphasizing transparency and user consent in European data protection terms, or notice and choice in United States parlance, the current legal framework imposes a burden on business and

[3] Peter Steiner, The New Yorker, 69(20), at p. 61, July 5, 1993.

[4] *See* generally Omer Tene, Privacy: The New Generations, 1 International Data Privacy Law 15 (2011), http://idpl.oxfordjournals.org/content/1/1/15.full. Online profiling may relate information not to an identified user but rather to an IP address, cookie or device. These, in turn, permit re-identification with various levels of difficulty. *See* Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy 111.

users which both parties struggle to lift. Users are ill placed to make responsible decisions about their online data, given, on the one hand, their cognitive biases and low stake in each data- (or datum-) transaction, and on the other hand, the increasing complexity of the online information ecosystem.[5] Indeed, even privacy professionals would be hard pressed to explain the inner-workings of the online market for personal information; the parties involved; and actual or potential uses of information. Imposing this burden on users places them at an inherent disadvantage and ultimately compromises their rights. It is tantamount to imposing the burden of health care decisions on patients instead of doctors

Granted, both sides of the online behavioral tracking debate may be guilty of policy laundering – the industry, for holding out users' vacuous, uninformed consent as a basis for depicting tracking as a voluntary practice; privacy advocates, for proposing opt-in rules in order to decimate the data-for-service value exchange. Instead of repeatedly passing the buck to users, the debate should focus on the limits of online behavioral tracking practices by considering which activities are socially acceptable and spelling out default norms accordingly. At the end of the day, it is not the size of the font in privacy notices or location of check-boxes in advanced browser settings which will legitimize or delegitimize online behavioral tracking. Rather, it is the boundaries set by policymakers, either in law, regulation or self-regulation,[6] for tracking practices based on their utility and relative intrusiveness.

The debate raging around online behavioral tracking generally and DNT in particular is a smoke screen for a discussion that all parties hesitate to hold around deeper values and social norms. Which is more important – efficiency or privacy;[7] law enforcement or individual rights;[8] reputation or freedom of speech?[9] Policymakers must engage with the underlying normative question: is online behavioral tracking a societal good, funding the virtue of the online economy and bringing users more relevant, personalized content and services;[10] or is it an evil scheme for

---

[5] For informative graphics *see* Before You Even Click, Future of Privacy Forum Blog, Apr. 29, 2010, www.futureofprivacy.org/2010/04/29/before-you-even-click; GCA Savvian, Display Advertising Technology Landscape: Dynamic Environment Ripe for Consolidation, May 3, 2010, http://www.adexchanger.com/pdf/Display-Advertising-Technology-Landscape-2010-05-03.pdf.

[6] Danny Weitzner, Associate Administrator at the National Telecommunications and Information Administration (NTIA), recently suggested the United States would seek a framework for online "privacy law without regulation." See Declan McCullagh, White House pledges new Net privacy approach, CNet, August 22, 2011, http://news.cnet.com/8301-31921_3-20095730-281/white-house-pledges-new-net-privacy-approach/#ixzz1WVK6sJFh.

[7] *See, e.g.,* Richard A. Posner, The Right of Privacy, 12 GA. L. REV. 393 (1978); George Stigler, An Introduction to Privacy in Economics and Politics, 9 J. LEGAL STUD. 623 (1980).

[8] *Cf.* Sharon H. Rackow, Comment, How the USA PATRIOT Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations, 150 U. PA. L. REV. 1651 (2002); and Orin Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 NW. U. L. REV. 607 (2003).

[9] *See, e.g.*, Mosley v. News Group Newspapers [2008] EWHC 1777 (QB).

[10] FTC Commissioner J. Thomas Rosch recently suggested "[t]he potential downsides of [regulatory initiatives include] the loss of relevancy, the loss of free content, the replacement of current advertising with even more intrusive advertising." Declan McCullagh, FTC commissioner calls for new 'do not track'

businesses to enrich themselves on account of ignorant users and for governments to create a foundation for pervasive surveillance? Policymakers cannot continue to sidestep these questions in the hope that "users will decide" for themselves.

Regardless of fine-tuning, the notice and choice mechanism presented to users will never be "value neutral" and balanced. The discussion among policymakers has been captured by debate of exactly how choice should be made; obsessed with the procedural mechanics of choosing (opt-in; opt-out; pre-checked box; forced choice; central opt-out; located on web page; linked to privacy policy; in browser; in advanced settings; etc.). The underlying premise is that "if users only knew – they would choose right". We argue that this is not a legitimate value-based proposition. Putting forth – "we do not have a position with respect to online behavioral tracking; our only position is that users should have a freedom to choose" – typically hides the real argument, which is "users should choose what *we* think is right for them".

The reason policymakers fail to reach consensus on transparency and choice is that such mechanisms are inherently skewed and always disguise a value judgment about the object of choice. Policymakers decided smoking is a social evil, imposing tremendous costs on the state and individuals; hence notices on cigarette packs are visceral (photo of emaciated lungs or dead bodies) and scolding ("cigarettes cause cancer"; "smoking can kill you").[11] Policymakers decided front seat passenger airbags should not be deactivated except after careful, premeditated deliberation; hence they disguised the disabling switch and permitted only authorized mechanics to perform the operation after customers execute liability release forms.[12] Policymakers decided unsolicited commercial communications (spam) did more harm (interruptions at dinner table; faxes sent in the middle of the night) than good (allowing small businesses to efficiently and cheaply market their goods and services) and therefore throttled this practice through burdensome opt-in requirements (in Europe) or a simple, centralized, prominent opt-out mechanism (in the United States).[13] If policymakers do not decide whether online behavioral tracking is a societal good or evil, they will never be able to settle the discussion about notice and choice.

In Part 2 we describe various online tracking technologies that have been implemented by industry to document, analyze and leverage browsing information. In Part 3 we describe the different purposes of online behavioral tracking and identify the parties involved. Part 4 lays out

---

approach, CNet, August 22, 2011, http://news.cnet.com/8301-31921_3-20095536-281/ftc-commissioner-calls-for-new-do-not-track-approach/#ixzz1WViQTVQx.

[11] Douglas Stanglin, FDA proposes graphic warnings for cigarette packs, USA Today, Nov. 10, 2010, http://content.usatoday.com/communities/ondeadline/post/2010/11/fda-proposes-graphic-images-and-warnings-for-cigarette-packages-and-ads/1.

[12] *See*, e.g., Heiko Johannsen et al, Misuse of Airbag Deactivation When Children are Travelling in the Front Passenger Seat, in Proceedings of the 21st International Technical Conference on the Enhanced Safety of Vehicles, June 2009, Stuttgart, Germany, http://www-nrd.nhtsa.dot.gov/pdf/esv/esv21/09-0351.pdf.

[13] The Telephone Consumer Protection Act, 47 U.S.C. § 227; The CAN-SPAM Act, 15 U.S.C. 7701, et seq., Pub. L. No. 108-187; FCC regulations implementing the CAN-SPAM Act, 47 C.F.R. § 64.3100.

the existing, albeit shifting, regulatory framework applicable to online behavioral tracking in the European Union, United States, and through industry self-regulatory initiatives. Part 5 addresses existing proposals for regulatory reform, including the FTC DNT scheme and initial industry response. In Part 6 we discuss our views on the state of current developments as well as the correct allocation of responsibility among users, businesses and policymakers. Part 7 concludes.

2. Online tracking devices

Online tracking technologies have been progressing rapidly, from cookies to "super cookies" (also known as "uber cookies"),[14] to browser fingerprinting and device identifiers. This enhanced tracking technology is made even more powerful by the "data deluge," or the age of "big data," that has dramatically lowered the cost of collection and storage of information. This powerful combination has motivated businesses to seek more innovative ways to manage and analyze heaps of data accumulated through various business processes.[15] In this Part, we describe the main tracking technologies, noting their relative transparency to users and how amenable they are for user control.

2.1. Cookies

Today, many people may be aware that their web browsing activity over time and across sites can be tracked using browser, or HTTP cookies.[16] Starting in the 1990s, cookies were initially

[14] Arvind Narayanan, Cookies, Supercookies and Ubercookies: Stealing the Identity of Web Visitors, 33 Bits of Entropy, Feb. 18, 2011, http://33bits.org/2010/02/18/cookies-supercookies-and-ubercookies-stealing-the-identity-of-web-visitors; Nicholas Jackson, The Next Online Privacy Battle: Powerful Supercookies, The Atlantic, August 18, 2011, http://www.theatlantic.com/technology/archive/2011/08/the-next-online-privacy-battle-powerful-supercookies/243800.

[15] The *Economist* recently reported that "the amount of digital information increases tenfold every five years." A special report on managing information: Data, data everywhere, The Economist, Feb. 27, 2010, http://www.economist.com/node/15557443; *see* discussion of government and private sector data mining in Ira Rubinstein, Ronald Lee & Paul Schwartz, Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, 75 U. Chi. L. Rev. 261 (2008).

[16] In fact, it is not even clear that this statement is true with respect to "plain vanilla" cookies (excuse the pun). In a series of empirical research projects, Joseph Turow, Chris Hoofnagle, Jennifer King and others have uncovered a striking degree of "privacy illiteracy" on the part of online users. For example, researchers found that users overvalue the mere fact that a website *has* a privacy policy, and assume that websites carrying the label have strong rules to protect personal data. Indeed, users interpret the existence of a "privacy policy" as a "quality seal" that denotes adherence to a set of acceptable standards. Chris Jay Hoofnagle & Jennifer King, What Californians Understand about Privacy Online, Sept. 3, 2008, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.161.5182&rep=rep1&type=pdf; *also see*

used to carry information between different web pages and offer re-identification of repeat visitors for usability reasons. Users, for example, preferred being presented with the time and weather in their hometown, compiling a shopping cart over time, and using personalized homepages over receiving generic untargeted data. By storing log-in credentials to various websites, cookies enabled users to revisit favorite websites without having to manage dozens of usernames and passwords.

Enhancements in the functionality of cookies provided websites and advertisers with a new means of collecting information about consumer interests and targeting ads on the basis of such information. When cookies were first utilized, information stored by cookies was not accessible to every website due to browser security policies. For example, "same-origin" policies allowed only the website that placed the cookie to read it. Such cookies, referred to as "first party cookies", created less of a privacy issue since they allowed a given website to track a user's activity strictly *on that site*. Subsequently, sharing of information between websites visited by a single user grew rapidly. Today, such information sharing techniques have become pervasive among popular websites, allowing users to be tracked in a multitude of ways. Tracking users across domains was enabled by cookies placed by third parties on many different websites belonging, for example, to an ad network.[17] An ad network typically places a cookie on a user's computer, which the network can subsequently recognize as the user moves from site to site. Using this identifier, the network can create a user profile based on the range of sites the user visits.[18] Increasingly, in a process known as "cookie synching," many third party cookies that ad networks and exchanges use are linked to enable the availability of data across multiple platforms, known as "cookie synching".[19] In addition, certain ad networks were reported to disregard user browser settings by relaying third party cookies in a first party context.

Joseph Turow, Lauren Feldman & Kimberly Meltzer, Open to Exploitation: American Shoppers Online and Offline, Annenberg Public Policy Center of the University of Pennsylvania, Jun. 1, 2005, http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31. Nevertheless, Turow, Hoofnagle and others report that 63% of online users, including 58% of users aged 18-24, regularly delete HTTP cookies. *See* Chris Hoofnagle, Jennifer King, Su Li and Joseph Turow, How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, Apr. 14, 2010, http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf.

[17] Alissa Cooper and Hannes Tschofenig recently observe that "a user's perception or expectation of the difference between a 'first party' and a 'third party' may not fall neatly within the distinction between 'first-party domain' and 'third-party domain.'" They present the example of a website sharing data with an analytics service provider using the same domain, although users may consider such a service provider to be a "third party"; conversely, users may expect to receive information via a social networking service from a photo-sharing service hosted at a different domain, while continuing to view the transaction as one performed with a single party. Alissa Cooper & Hannes Tschofenig, Overview of Universal Opt-Out Mechanisms for Web Tracking, Network Working Group, Mar. 7, 2011 , http://tools.ietf.org/html/draft-cooper-web-tracking-opt-outs-00.

[18] *See* extensive discussion in Statement of Federal Trade Commission concerning Google/DoubleClick, In re Google and DoubleClick, Federal Trade Commission File No. 071-0170 (F.T.C. Dec. 21, 2007), http://ftc.gov/os/caselist/0710170/071220statement.pdf.

[19] Cookie Synching, Krux Digital Blog, Feb. 24, 2010, http://blog.kruxdigital.com/2010/02/24/cookie-synching.

Such "third party," or "tracking" cookies, drew criticism from privacy advocates and prompted lawsuits alleging computer fraud, wiretapping and privacy violations.[20] Although these lawsuits were largely unsuccessful, browser makers were incentivized to continue to improve privacy controls that gave users an increased ability to limit and delete cookies. Browsers provided users a degree of control over cookies, allowing them to block all cookies, or only those cookies that were shared with third parties; to selectively enable or disable cookies on a site-by-site basis; or to allow cookies for a website generally but delete a specific cookie they found objectionable.

Few users bother to actively manage their cookie settings, beyond, perhaps, periodically emptying the cookie folder on their machine.[21] Nevertheless, websites are relatively transparent with respect to their first and third party cookie policies, particularly when compared to other tracking devices. This allows users to exert choice to manage cookie settings or avoid downloading cookies altogether.

2.2. Flash Cookies

Recent news reports,[22] as well as class action lawsuits,[23] alleged online advertisers misused Flash cookies, or "local shared objects," to store information about users' web browsing history, employing Flash cookies in a way unrelated to the delivery of content through the Flash Player.

As a tracking mechanism, Flash cookies offer online advertisers several advantages *vis-à-vis* HTTP cookies. First, Flash cookies can contain up to 100KB of information by default, compared to 4KB by HTTP cookies. Second, Flash cookies do not have expiration dates by default, whereas HTTP cookies expire at the end of a session unless programmed otherwise. Third, unlike HTTP cookies, which can be managed simply by changing browser settings, Flash cookies are stored in a separate directory that many users are unaware of and do not know how to control. Indeed, a

[20] In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003); dismissed on remand, 292 F. Supp. 2d 263 (D. Mass. 2003); In re DoubleClick, Inc., Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[21] Magid Abraham, Cameron Meierhoefer & Andrew Lipsman, The Impact of Cookie Deletion on the Accuracy of Site- Server and Ad-Server Metrics: An Empirical Comscore Study, 2007, http://www.comscore.com/Press_Events/Presentations_Whitepapers/2007/Cookie_Deletion_Whitepaper.

[22] Ryan Singel, You Deleted Your Cookies? Think Again, Wired, August 10, 2009, http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again.

[23] Tanzina Vega, Code That Tracks Users' Browsing Prompts Lawsuits, NY Times, Sept. 20, 2010, http://www.nytimes.com/2010/09/21/technology/21cookie.html; *see* Rona v. Clearspring Techs., Inc., No. 2:10-cv-07786-GW-JCG (C.D. Cal.) (filed Oct. 18, 2010); Godoy v. Quantcast Corp., No. 2:10-cv-07662 (C.D. Cal.) (filed Oct. 13, 2010); Davis v. VideoEgg, Inc., No. 2:10-cv-07112-GW-JCG (C.D. Cal.) (filed Sept. 23, 2010); Intzekostas v. Fox Entm't Group, No. 2:10-cv-06586-GW-JCG (C.D. Cal.) (filed Sept. 2, 2010); La Court v. Specific Media, Inc., No. 8:10-cv-01256-JVS-VBK (C.D. Cal.) (filed Aug. 19, 2010); White v. Clearspring Techs., Inc., No. 2:10-cv-05948-GW-JCG (C.D. Cal.) (filed Aug. 10, 2010); Aguirre v. Quantcast Corp., No. 2:10-cv-05716-GW-JCG (C.D. Cal.) (filed July 30, 2010); Valdez v. Quantcast Corp., No. 2:10-cv-05484-GW-JCG (C.D. Cal.) (filed July 23, 2010).

number of lawsuits contended that online advertisers used Flash cookies to collected information about users' web browsing to circumvent those users' choice to set their browser to reject cookies. Erasing HTTP cookies, clearing history, erasing the cache, or even using the "Private Browsing" mode added to most browsers, still allowed Flash cookies to operate fully. Finally, and most disturbing, Flash cookies were alleged to have been used for "respawning"– the practice of restoring deleted HTTP cookies, thereby overriding users' express choice to limit third party tracking.[24]

These differences make Flash cookies a more resilient and intrusive tracking technology than HTTP cookies, and create an area of uncertainty for user control not only of Flash but also of HTTP cookies. Fortunately, Flash software maker Adobe Systems has recently addressed this alleged misuse by coordinating its application programming interface (API) with browser companies so that by deleting HTTP cookies users will also clear their Flash cookies.[25] A follow-up research by Aleecia McDonald and Lorrie Cranor found little evidence of websites using Flash functionality to respawn HTTP cookies.[26]

While Flash cookies have been the focus of litigation, similar tracking results can be obtained with other types of local storage such as Microsoft's Silverlight framework,[27] HTML 5 databases,[28] and ETags.[29] The new web language and its additional features present more tracking opportunities because the technology uses a process in which large amounts of data

[24] Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas & Chris Jay Hoofnagle, Flash Cookies and Privacy, Aug. 10, 2009, http://ssrn.com/abstract=1446862.

[25] Emmy Huang, On Improving Privacy: Managing Local Storage in Flash Player, Adobe Flash Platform Blog, Jan. 12, 2011, http://blogs.adobe.com/flashplatform/2011/01/on-improving-privacy-managing-local-storage-in-flash-player.html. Ms. Huang announced: "Representatives from several key companies, including Adobe, Mozilla and Google have been working together to define a new browser API (NPAPI ClearSiteData) for clearing local data, which was approved for implementation on January 5, 2011. Any browser that implements the API will be able to clear local storage for any plugin that also implements the API." However, she admits: "Still, we know the Flash Player Settings Manager could be easier to use, and we're working on a redesign coming in a future release of Flash Player, which will bring together feedback from our users and external privacy advocates. Focused on usability, this redesign will make it simpler for users to understand and manage their Flash Player settings and privacy preferences." *See* discussion of transparency tools *infra.*

[26] Aleecia McDonald & Lorrie Cranor, A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies, Jan. 31, 2011, http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11001.pdf.

[27] Dan Goodin, IE is tough on Flash cookies but ignores homegrown threat, The Register, May 5, 2011, http://www.theregister.co.uk/2011/05/05/silverlight_privacy_menace.

[28] *See infra* notes 35–36 and accompanying text.

[29] *See* Mika Ayenson, Dietrich Wambach, Ashkan Soltani, Nathan Good & Chris Hoofnagle, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, July 29, 2011, Working Paper, http://ssrn.com/abstract=1898390; *also see* Wendy Davis, Privacy Advocates Ask FTC to Condemn New Tracking Methods, MediaPost News, August 23, 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=157305.

can be collected and stored locally on users' machines, while users have little transparency and control with respect to such data collection and use.[30]

2.3. Browser fingerprinting

Initially deployed by banks to prevent identity fraud or by software companies to preclude illegal copying of computer software, browser fingerprinting also is a powerful technique for tracking online users. By gathering seemingly innocuous bits of information, such as a browser's version number, plug-ins, operating system and language, websites can uniquely identify ("fingerprint") a browser and by proxy, its user.[31] Not only do browser fingerprints track users more accurately than cookies, they are also harder to detect and control than predecessor technologies.[32] In addition, users do not have tools at their disposal for making a browser more anonymous.

In a comprehensive study, the Electronic Frontier Foundation (EFF) found that while some browsers are less likely to contain unique configurations, such as those that block JavaScript, and some browser plug-ins may be configured to limit the information a browser shares with the websites a user visits, it remains very difficult to reconfigure a browser to make it less identifiable. Even sophisticated web users would need to strain to verify whether their browser is being fingerprinted. And while users may purposefully modify their configuration, adding or deleting fonts, or updating software, trackers would still recognize them. Hence, fingerprinting is largely invisible, difficult to fend off and semi-permanent.

Although the use of browser fingerprinting by industry for advertising or tracking is still nascent, early business models are starting to emerge.[33]

---

[30] Tanzina Vega, New Web Code Draws Concern Over Privacy Risks, NY Times, Oct. 10, 2010, http://www.nytimes.com/2010/10/11/business/media/11privacy.html?_r=1&src=busln.

[31] Peter Eckersley How Unique Is Your Web Browser?, Electronic Frontier Foundation (2010), https://panopticlick.eff.org/browser-uniqueness.pdf. For device fingerprinting in another age, *see* Ordway Hilton, The Complexities of Identifying the Modern Typewriter, 17(2) J. Forensic Sciences (1972); *also see* Julia Angwin & Jennifer Valentino-Devries, Race Is On to 'Fingerprint' Phones, PCs ("What They Know series"), Wall Street Journal, Nov. 30, 2010, available at http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html.

[32] *See*, e.g., Rona v. Clearspring Techs., Inc., No. 2:10-cv-07786-GW-JCG (C.D. Cal.) (filed Oct. 18, 2010); Godoy v. Quantcast Corp., No. 2:10-cv-07662 (C.D. Cal.) (filed Oct. 13, 2010); Davis v. VideoEgg, Inc., No. 2:10-cv-07112-GW-JCG (C.D. Cal.) (filed Sept. 23, 2010)

[33] Julia Angwin & Jennifer Valentino-Devries, Race Is On to 'Fingerprint' Phones, PCs, Wall Street Journal, Nov. 30, 2010, http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html. *See*, e.g., Blue Cava website, stating: "We target online advertising better. And we help fight fraud. With increasing frequency these days companies are saying to us: 'Hey, that's really great technology. I bet I can use it for (fill in the blank with something interesting'). In the center of BlueCavaland is our patented device identification technology that generates unique fingerprints for any internet connected electronic device. Our universe is big. Like 10 Billion devices in the world big. That's our sandbox." http://www.bluecava.com.

2.4. Mobile devices

Mobile browsing is expected to surpass fixed internet use in the next few years, rendering the tracking of users of mobile devices, including phones and tablets, increasingly important.[34] Mobile browsing differs from fixed browsing in two significant ways: First, users carry their mobile device with them at all times, allowing ad intermediaries to track not only their browsing activity but also their physical location; indeed, few devices store more personal details about their users than mobile phones, including contact numbers, location, and a unique identifying number that cannot be changed or turned off.[35] Second, mobile users consume online services by downloading applications ("apps"), software programs that allow them to play games, read e-books, or search for restaurants without launching a browser or using a search engine. Mobile apps thus replace browsers and search engines as the main entry gate to the mobile internet.

In a recent lawsuit, plaintiffs claimed the defendant company used an HTML5 storage database on users' mobile devices to store an assigned unique identifying number in order to track users across websites for advertising purposes.[36] Indeed, the defendant still openly declares on its website that its main product "is the mobile equivalent of an online 'cookie'" that "seamlessly integrates with existing digital advertising platforms to share unique ID information… [letting] you identify and track unique mobile and new media users to leverage ad server functionality…"[37] Plaintiffs claimed that even in the unlikely case that users found and deleted the HTML5 database, it would soon repopulated with identical identifying information.

In another case, Federal prosecutors in New Jersey launched an investigation to check whether mobile apps illegally obtained and transmitted information about their users, including users' location and device unique identifiers, without proper disclosure. Investigators examined whether app makers fully described to users the types of information they collected and what

[34] *See* Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy, Hearing before Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, May 10, 2011, http://judiciary.senate.gov/hearings/hearing.cfm?id=5157.

[35] *See* Yukari Iwatani Kane, Apple Shuns Tracking Tool, Wall Street Journal, August 19, 2011, http://online.wsj.com/article/SB10001424053111903639404576519101872716410.html#ixzz1WVPDOpzG; Article 29 Data Protection Working Party Opinion on Geolocation services on smart mobile devices, WP 185, May 16, 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf; MSISDN, Wikipedia, http://en.wikipedia.org/wiki/MSISDN; International Mobile Equipment Identity, Wikipedia, http://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity. Moe Rahnema, Overview of the GSM system and protocol architecture, 31(4) Communications Magazine, IEEE 92 (1993).

[36] Aughenbaugh v. Ringleader Digital, Inc., No. 8:10-cv-01407-CJC-RNB (C.D. Cal.) (filed Sept. 16, 2010). *See* David Kravets, Lawsuit Targets Mobile Advertiser Over Sneaky HTML5 Pseudo-Cookies, Wired, Sept. 16, 2010, http://www.wired.com/threatlevel/2010/09/html5-safari-exploit.

[37] Ringleader Digital website, http://www.ringleaderdigital.com/our-platform/media-stamp.

they would be used for.[38] In the same vein, the *Wall Street Journal* reported that an examination of 101 popular apps revealed that 56 of the apps transmitted user phones' unique device IDs to third parties without the users' awareness or consent. Forty-seven apps transmitted the phones' location; and five sent age, gender and other personal information to third party advertisers.[39] The *Wall Street Journal* reported that "A growing industry is assembling this data into profiles of cellphone users."[40]

In the mobile app economy, compliance with privacy expectations is irregular and highly unpredictable. On the one hand, many app makers are small software developers– even garage-based teenagers writing code, who are judgment-proof and hardly attuned to privacy regulation. On the other hand, allocating liability to app intermediaries such as operating system makers (namely Google and Apple) or to mobile operators raises thorny issues given the daunting difficulties such intermediaries would face if required to screen the privacy or indeed any policies of the hundreds of thousands of mobile apps they host. The logic underpinning the blanket immunity granted to online intermediaries under Section 230 of the Communications Decency Act[41] applies in similar force here. Intermediary liability would stifle innovation, restrict free speech, raise antitrust concerns and dampen the online economy.

The upshot of all this is that users of the mobile internet are subject to opaque data collection and use practices by multiple parties, many of them obscure to users and largely insulated from regulation. Transparency and user control are very low.[42]

2.5. Deep Packet Inspection

One technology that has created significant concern when used for online behavioral tracking is deep packet inspection (DPI). Initially employed by internet service providers (ISPs) for security and maintenance,[43] DPI has emerged as a new tool utilized by advertising companies to categorize all of the websites a user visited in order to tailor banner ads.[44] The President of the

[38] Amir Efrati, Scott Thurm & Dionne Searcey, Mobile-App Makers Face U.S. Privacy Investigation, Wall Street Journal, Apr. 5, 2011, http://online.wsj.com/article/SB10001424052748703806304576242923804770968.html.
[39] Scott Thurm & Yukari Iwatani Kane, Your Apps Are Watching You, Wall Street Journal, Dec. 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.
[40] Ibid.
[41] 47 U.S.C. § 230.
[42] For example, to opt-out of mobile ad targeting at many mobile ad networks, users are required to both accept an opt-out cookie and provide their unique device identifier (UDID).
[43] Angela Daly, The legality of deep packet inspection, in the First Interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade', University of Glasgow 17 June 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024.
[44] Saul Hansell, I.S.P. Tracking: The Mother of All Privacy Battles, NY Times, Mar. 20, 2008, http://bits.blogs.nytimes.com/2008/03/20/the-mother-of-all-privacy-battles; Steve Stecklow & Paul

Center for Democracy and Technology (CDT) Leslie Harris likens it to "postal employees opening envelopes and reading the letters inside."[45]

DPI would give advertisers the ability to show ads to people based on extremely detailed profiles of their online activity. Indeed, by partnering with ISPs, ad networks would potentially gain access to profiles based on a wide view of an individual's online traffic as it travels through the ISP's infrastructure. Some have argued that traditional ad networks have very broad access to users' web surfing, and when additional data from data exchanges is brought into the process they too may have an extraordinarily wide view of a user's activity;[46] yet the backlash against DPI-based ad targeting led to leading United States ISPs publicly committing to only using such an advertising model with consumer consent.[47] As a result, the leading United States company in this business, NebuAd, went out of business.[48] Meanwhile Phorm, the company that kicked off the controversy over DPI in the United Kingdom,[49] is now publicly active only in Korea and Brazil and has proposed an opt-in model for its services in the United States with little success to date.[50]

2.6. History sniffing

Additional online tracking technologies exist and more will likely gain prevalence taking into consideration the ever increasing value of user data. For example, a lawsuit was recently filed alleging websites and ad intermediaries used "history sniffing" to surreptitiously detect what

---

Sonne, Shunned Profiling Technology on the Verge of Comeback, Wall Street Journal, Nov. 24, 2010, http://online.wsj.com/article/SB10001424052748704243904575630751094784516.html.

[45] Center for Democracy & Technology, Statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology, Before the House Committee on Energy and Commerce, Subcommittee on Communications, Technology and the Internet, "The Privacy Implications of Deep Packet Inspection", Apr. 23, 2009, http://www.cdt.org/privacy/20090423_dpi_testimony.pdf.

[46] Balachander Krishnamurthy & Craig Wills, Privacy diffusion on the web: A longitudinal perspective, In Procs World Wide Web Conference, Madrid, Spain (April 2009), http://www.research.att.com/~bala/papers/www09.pdf, reporting Google "family" (including Doubleclick, Google Analytics, etc.) present on circa 60% of all websites (as of September 2008).

[47] Sam Diaz, ISPs keep their distance from deep packet inspection, ZDNet, Sept. 25, 2008, http://www.zdnet.com/blog/btl/isps-keep-their-distance-from-deep-packet-inspection/10166 ("Testimony this morning from AT&T, Verizon and Time Warner Cable executives were all very similar: we respect our customers privacy, customers should be given an opt-in- not opt-out - choice").

[48] Wendy Davis, Embarq Wins Privacy Suit Stemming From NebuAd Tests, MediaPost News, August 23, 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=156350; Scott Austin, Turning Out the Lights: NebuAd, WSJ Blogs, May 19, 2009, http://blogs.wsj.com/venturecapital/2009/05/19/turning-out-the-lights-nebuad.

[49] Chris Williams, BT admits misleading customers over Phorm experiments, The Register, Mar. 17, 2008, http://www.theregister.co.uk/2008/03/17/bt_phorm_lies.

[50] Jack Marshall, Phorm Shifts Focus to Brazil, Posts First Revenues, ClickZ, July 1, 2010, http://www.clickz.com/clickz/news/1721855/phorm-shifts-focus-brazil-posts-first-revenues.

websites a user has visited by running code inside such user's browser.[51] Browser history sniffing exploits the functionality of browsers that display hyperlinks of visited and non-visited sites in different colors (blue for unvisited sites; purple for visited). A website is allowed to query a user's browser history in order to know what color to render the links displayed on its web pages. Websites apparently gamed this functionality by running Javascript code in order to list hundreds of URLs, thereby recreating a user's browsing history – all without the user's knowledge or consent.[52] Apple's Safari was the first major browser to insulate users against this threat, soon to be followed by Google Chrome as well as beta versions of Mozilla Firefox and Microsoft Internet Explorer.[53]

3. Uses of tracking

The collection, retention, use and transfer of information about online users come in many guises. Increasingly large amounts of data are posted online voluntarily by users themselves, on social networking services, web forums, blogs and personal web pages. The harvesting and use of such data, while raising significant privacy issues, are beyond the scope of tracking discussed in this paper.[54] The paradigmatic tracking activity we examine involves **a third party largely unfamiliar to the user collecting and processing information about her based on her browsing activity on various unrelated websites in order to compile an individual profile, which will be used to facilitate the targeting of ads**.[55] We call this type of activity, which studies indicate has created an uneasy feeling among many users, "online behavioral tracking".[56]

---

[51] Jonathan Mayer, Tracking the Trackers: To Catch a History Thief, Stanford CIS Blog, July 19, 2011, http://cyberlaw.stanford.edu/node/6695; Kashmir Hill, History Sniffing: How YouPorn Checks What Other Porn Sites You've Visited and Ad Networks Test The Quality of Their Data, The Not-So Private Parts, Nov. 30, 2010, 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; Jessica E. Vascellaro, Suit to Snuff Out 'History Sniffing' Takes Aim at Tracking Web Users, Wall Street Journal, Dec. 6, 2010, http://online.wsj.com/article/SB10001424052748704493004576001622828777658.html.

[52] Dongseok Jang, RanjitJhala, Sorin Lerner & Hovav Shacham, An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications, in ACM Conference on Computer and Communications Security (CCS), 2010. http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf; Zack Weinberg, Eric Chen, Pavithra Ramesh Jayaraman & Collin Jackson, I Still Know What You Visited Last Summer: Leaking browsing history via user interaction and side channel attacks, in Proc. of the IEEE Security and Privacy Symposium (Oakland 2011), http://websec.sv.cmu.edu/visited/visited.pdf.

[53] *See* L. David Baron, Preventing attacks on a user's history through CSS: visited selectors, Mozilla Corporation, Mar. 9, 2010, http://dbaron.org/mozilla/visited-privacy.

[54] *See* Julia Angwin and Steve Stecklow, 'Scrapers' Dig Deep for Data on Web, Wall Street Journal, Oct. 12, 2010, http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html; Facebook v. Power Ventures, Case No. 5:08-cv-05780 JW (N.D. Cal.).

[55] The CDT offered the following definition of "tracking": "Tracking is the collection and correlation of data about the Internet activities of a particular user, computer, or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or compliance with law

In order to maintain a stable equilibrium between user expectations and the legitimate needs of online businesses, the market must reinforce mechanisms for transparency and user control over online behavioral tracking, while at the same time not overly impeding the fundamental business model of the internet economy, financing products and services by targeted ads. In a recent research paper, Howard Beales, former Director of the Bureau of Consumer Protection at the FTC, asserted that the price of behaviorally targeted advertising was 2.68 greater than the price of untargeted ads.[57] In addition, the same data used for online behavioral tracking is also collected for less privacy sensitive purposes distinct from targeted advertising, such as enhancing user experience, measuring effective exposure, and preventing fraud and misconduct.[58] We briefly discuss these additional tracking activities below.

3.1. First party tracking

A website needs to know basic information about its users, most notably their IP address, to be able to deliver content to them. Websites track users to support billing, complete online transactions, personalize user experience and website design, provide product recommendations and shopping cart services, tailor content and target their own products or services. For example, when a user signs on to Amazon and enters a username and password, the system will match that sign-on information to saved preferences thus personalizing the experience for that user, maintaining her shopping cart and providing personalized product recommendations.

3.2. Analytics

Many website owners use third-party analytics tools to evaluate traffic on their own websites. These tools allow websites to compile a comprehensive set of statistics about visitors, including how often they visit, their domains and countries of origin, what pages they view the most, and which operating system and browser they use to access the website. Google Analytics, for

---

enforcement requests." Justin Brookman, What Does "Do Not Track" Mean?, A Scoping Proposal by the Center for Democracy & Technology, Jan. 31, 2011, http://www.cdt.org/files/pdfs/CDT-DNT-Report.pdf.

[56] *See* Joseph Turow, Jennifer King, Chris Hoofnagle, Amy Bleakley and Michael Hennessy, Americans Reject Tailored Advertising and Three Activities that Enable It, Sept. 29, 2009, http://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers; reporting that that 66% of adults in the United States do not want websites to show them tailored advertising; 75% do not want ads based on websites they visit; 87% do not want ads based on websites they have visited.

[57] Howard Beales, The Value of Behavioral Targeting, study sponsored by the Network Advertising Initiative, Mar. 24, 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[58] The self-regulatory principles proposed by the Federal Trade Commission also exclude from their scope any non-advertising behavioral targeting (at p. 20); contextual advertising (at p. 28); first party tracking (at p. 26).

example, states it offers "easy-to-understand reports to make measurable improvements to campaigns and websites. Learn which keywords, sites and locations bring high-value traffic, and be more informed about how visitors are reacting to your site's content."[59] The CDT observes that while conducted by a third party, the information delivered to the first party website is exclusively about traffic on that site, which means that such activity does not constitute online behavioral tracking. Indeed, many *offline* businesses use third party service providers to collect, analyze and maintain data about usage of their products and services. Assuming service providers ("processors" in European data protection parlance) comply with basic requirements of data security and purpose limitation, such activity is not considered to expose customers to privacy risks.[60] Moreover, many leading analytics providers allow end users to opt-out of online measurement.[61]

3.3. Measurement

Given that the online ecosystem is supported by advertising, websites, advertisers and ad intermediaries must use various tools to measure user engagement and the effectiveness of ad campaigns. Such tools log page views, visits, unique visitors, entry and exit pages, referrers and clickthrough rates, to facilitate accounting among the multiple parties to online transactions. In addition, tracking is also used for "frequency capping", or ensuring that the same ad is not shown repeatedly to a given browser or user.

Measurement is undertaken for two major purposes. The first is to confirm to advertisers the delivery and posting of their advertisements according to contracted schedules by providing related posting states, data, and reports. The other is to help advertisers collect the data about advertisement posting, audience viewing and access, which will be useful for performance analysis and measurement of advertisements.

Regardless of the ongoing debate surrounding the desired scope of online tracking, almost all websites featuring ads would be adversely impacted if data collection for measurement purposes was curtailed. However, many ad networks use the same cookie for web measurement that they do for online behavioral tracking, so the opt-out they provide for tracking does limit collection for measurement as well. Given that historic opt-out rates are estimated at less than one percent of all users, ad networks have been able to provide users

[59] http://www.google.com/intl/en_us/services/var_1.html.
[60] *See*, e.g., Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Feb. 16, 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf; Article 29 Data Protection Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Nov. 22, 2006, WP 128, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.
[61] *See*, e.g., Webtrends (http://www.webtrends.com), comScore (http://www.comscore.com),Omniture (http://www.omniture.com/en).

with this choice without significantly impacting measurement needs.[62] Significantly higher opt-out rates would be likely to upset the basic business model.

In a joint report, the CDT and EFF distinguish between web measurement, which is confined to reporting results in the aggregate, and web analytics, which covers a broader space of practices that may involve reporting individual-level data. The CDT and EFF note that the risk of re-identifying an individual user based on only the reported aggregate measurement data is negligible, and that any individual-level data collected for the purpose of measurement is retained only for a limited time period.[63]

3.4. Network security

Websites and ISPs have multiple reasons to log and track the traffic that comes through their systems, including limiting malicious activity, such as denial of service attacks, viruses and spam;[64] managing online traffic;[65] and cooperating with copyright holders concerned about illegal access to proprietary material.[66]

---

[62] Joe Mullin, Less Than 1 Percent of Firefox Users Using 'Do Not Track' Option, PaidContent.org, Apr. 22, 2011, http://paidcontent.org/article/419-less-than-1-of-firefox-users-using-do-not-track-option; Google disclosed that of those users who encounter its ad preferences manager and opt-out interface (ostensibly, the more privacy-conscious users), under 7% elect to opt-out of tracking; 28% edit their profile; and the remainder do nothing. *See* Zachary Rodgers, Few Google Users are Opting Out of Behavioral Targeting, Dec. 13, 2009, http://www.clickz.com/clickz/news/1709106/few-google-users-are-opting-out-behavioral-targeting; MediaPost reports: "Evidon had served over 11 billion impressions. Among those who click on the icon (at a .004% rate), about 3% are opting out of one or more provider. 'That translates to over 450,000 consumers who have clicked through on icons served by Evidon in four months of production at scale,' he tells me. 'Of those, approximately 15,000 have requested opt-outs through our platform, with each consumer making an opt-out decision frequently requesting opt-out from more than one company'." Steve Smith, Browsing Privacy's Next Steps, MediaPost, Mar. 11, 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=146581.

[63] Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites, Center for Democracy & Technology, Electronic Frontier Foundation, May 2009, http://www.cdt.org/privacy/20090512_analytics.pdf.

[64] Christopher Soghoian, Security and Fraud Exceptions Under Do Not Track, Center for Applied Cybersecurity Research, Indiana University, Position Paper for W3C Workshop on Web Tracking and User Privacy, April 28-29, 2011, Princeton, http://www.w3.org/2011/track-privacy/papers/Soghoian.pdf.

[65] Charles Jackson, Wireless Efficiency versus Net Neutrality, 63 Fed. Comm. L.J. 445 (2011); C. Scott Hemphill, Network Neutrality and the False Promise of Zero-Price Regulation, 25 Yale J. Reg. 135 (2008).

[66] But *see* recently: Belgian ISP does not have to filter out copyright-infringing traffic, says ECJ advisor, OutLaw, Apr. 14, 2011, http://www.out-law.com//default.aspx?page=11869&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+out-law-NewsRoundUP+%28OUT-LAW+News-RoundUP%29; Advocate General of the European Court of Justice submitting that ISP monitoring of online content for copyright infringement violates rights guaranteed under EU law: "The installation of the filtering and blocking system is a restriction on the right to respect for the privacy of communications and the right to protection of personal data, both of which are rights protected under the Charter of Fundamental Rights."

3.5. Fraud prevention and law enforcement

Various laws and regulations allow or even and require websites and online intermediaries to track users and maintain profiles for purposes of fraud prevention, anti-money laundering, national security and law enforcement. In the European Union, for example, "providers of publicly available electronic communications services or of a public communications network" must retain "traffic data and location data and the related data necessary to identify" subscribers or users for a period no less than six to twenty-four months.[67] Similar requirements are imposed by anti-money laundering legislation with respect to banks and financial institutions.[68] Hence, for example, banks are required to implement authentication systems, which log user interaction to verify the identity of customers accessing their accounts through online platforms.[69]

Government can conduct its own sort of third party tracking of online activities using law enforcement or national security powers.[70] In addition, government may use legal process to access online tracking information collected by commercial entities including websites and ISPs.[71] Google has recently posted a map reporting the number of government requests it

[67] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 (April 13, 2006), Article 6. *See* generally Francesca Bignami, Privacy and Law Enforcement in the European Union: The Data Retention Directive, 8 Chi. J. Int'l L. 233, 238 (2007).

[68] *See*, e.g., in Europe: Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; Council Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering [91/308/EEC]; in the United States: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

[69] Mark MacCarthy, Information Security Policy in the U.S. Retail Payments Industry, 2011 Stan. Tech. L. Rev. 3;Ritu Sing, Two-Factor Authentication: A Solution to Times Past or Present? The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance, 2 I/S: J. L. & Pol'y for Info. Soc'y 761 (2006);

[70] *See*, e.g., in the United States: Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994), codified at 47 U.S.C. §§1001-10; in the United Kingdom: Regulation of Investigatory Powers Act 2000, c. 23.

[71] *See* recently: American Civil Liberties Union, Legal Battle Over Government Demands For Twitter Records Unsealed by Court, ACLU Blog, Feb. 8, 2011, http://www.aclu.org/free-speech/legal-battle-over-government-demands-twitter-records-unsealed-court; *also see* Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006); Omer Tene, What Google Knows: Privacy and Internet Search Engines, 2008 Utah L. Rev. 1433.

receives for data about the use of Google services around the world.[72] Moreover, government has been known to acquire massive amounts of personal data from commercial data brokers.[73]

4. Regulating Online Tracking

The regulatory framework for both online and offline privacy is currently in flux. Although modeled to be technologically neutral and apply across industries, it is strained by a sea change of innovation and breakthroughs, leading to an urgent need for reform. Nowhere is this more evident than in the online environment, which was merely in its infancy when the regulatory framework was put in place. This led governments, regulators and industry leaders in the European Union and United States to introduce new regulatory and self-regulatory frameworks applicable to online behavioral tracking. We review these measures below.

4.1. Europe

In Europe, the legal framework applying to online behavioral tracking consists of the European Data Protection Directive,[74] which regulates the collection, processing, storage and transfer of personal data; and the European e-Privacy Directive,[75] which regulates data privacy on communication networks. The Data Protection Directive sets forth basic principles such as notice; consent; proportionality; purpose limitation; and retention periods; which apply not only online but also to offline data collection and use. The e-Privacy Directive protects, among other things, the confidentiality of communications; spam; traffic and location data; and specifically addresses the use of cookies.[76]

---

[72] Google Transparency Report, Government Requests, www.google.com/transparencyreport/governmentrequests.

[73] Michael Birnhack & Niva Elkin-Koren, The Invisible Handshake: The Reemergence of the State in the Digital Environment, 8 VA. J. L. & TECH. 6 (2003); Chris Jay Hoofnagle, Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J. INT'L L. & COM. REG. 595 (2004).

[74] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), transposed in the United Kingdom, for example, via the Data Protection Act 1998, c. 29.

[75] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. L 201, 31.7.2002, p. 37–47, transposed in the United Kingdom, for example, via the Privacy and Electronic Communications (EC Directive) Regulations 2003, No. 2426.

[76] e-Privacy Directive, Recital 25. The Information Commissioner's Office (ICO), the United Kingdom's privacy regulator, recently clarified that the scope of the e-Privacy Directive is not restricted to HTTP cookies but rather applies to additional tracking technologies, such as Flash cookies. Information Commissioner's Office, Changes to the rules on using cookies and similar technologies for storing information, May 9, 2011,

Article 5(3) of the e-Privacy Directive previously stated: "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller." This provision required transparency on behalf of websites or third parties placing cookies on a user's computer and applied an opt-out rule ("right to refuse") with respect to user consent. Based on the way that this requirement was transposed into the law of most Member States, industry took the language to mean that it was acceptable to give users the ability to reject a cookie *after* it had been delivered. Accordingly, websites generally included in their privacy policies instructions for disabling or rejecting cookies.

However, in December 18, 2009, the e-Privacy Directive was amended as part of the "Telecoms Reform Package" of legislation.[77] Article 5(3) now reads: "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, *inter alia*, about the purposes of the processing." The new language, which comes into force across Europe on May 25, 2011, appears to call for opt-in consent[78] to the storage of or access to a cookie on a user's computer.[79] Yet clearly this is impractical, given that many websites now post dozens – in some cases hundreds –

---

http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf.

[77] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. This Directive entered into force on the day following its publication in the Official Journal of the European Union, i.e., on December 19, 2009. According to Article 4(1), Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with the Directive by May 25, 2011. That is the time that amended Article 5(3) of the e-Privacy Directive comes into force across Europe.

[78] Consent is defined in Article 2(h) of the Data Protection Directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

[79] Notice that Article 5(3) applies not only to the use of cookies but also to any information stored on users' terminal equipment via an electronic communications network or via external data storage media, such as CD-ROMs or USB sticks. Moreover, Article 5(3) applies to the storing of information, regardless of whether this information constitutes "personal data" under the Data Protection Directive. *Cf*. Recital 24 of the e-Privacy Directive stating that "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms".

of cookies to a user's computer,[80] ostensibly requiring the user to incessantly click through "I accept" pop-up windows on each web page she visits.[81]

One potential avenue for minimizing the impact of the stringent consent requirement in the new Article 5(3) appears in Recital 66 to the e-Privacy Directive, which states: "Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[82] Hence, in addition to permitting the use of a cookie without opt-in consent where such a cookie is needed to carry out a service that the user has clearly requested,[83] Recital 66 appears to authorize the use of browser settings to signify consent to cookies.[84]

However, in June 2010, the Article 29 Working Party (the group of European privacy regulators charged with interpreting and enforcing the law) published an opinion analyzing the language of amended Article 5(3) and the interplay between it and Recital 66 of the e-Privacy Directive, and insisting that anyone who wants to engage in online behavioral tracking must first obtain users' affirmative opt-in consent.[85] The Working Party rejected an opt-out approach, concluding that it

---

[80] Julia Angwin, The Web's New Gold Mine: Your Secrets, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[81] For a demonstration *see* David Naylor, EU "Cookies" Directive. Interactive guide to 25th May and what it means for you, David Naylor Blog, http://www.davidnaylor.co.uk/eu-cookies-directive-interactive-guide-to-25th-may-and-what-it-means-for-you.html.

[82] "The Recitals are the part of a legal act on EU level which contains the statement of reasons for the act; they are placed between the citations and the enacting terms. The statement of reasons begins with the word "whereas" and continues with numbered points comprising one or more complete sentences. It uses non-mandatory language and must not be capable of confusion with the enacting terms." Joint Practical Guide, Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of legislation within the Community institutions. http://eur-lex.europa.eu/en/techleg/10.htm. *Also see* Tadas Klimas & Jurate Vaiciukaite, The Law of Recitals in European Community Legislation, 15 ILSA Journal of International & Comparative Law 1(2008).

[83] The UK ICO recently rejected the use of this exception "if you decide to use a cookie to collect statistical information about the use of your website." Hence, use of cookies for measurement or analytics appears to require opt-in consent. The ICO explained: "This exception needs to be interpreted quite narrowly because the use of the phrase 'strictly necessary' means its application has to be limited to a small range of activities and because your use of the cookie must be related to the service requested by the user." ICO Guidance, *supra* note 76, at p. 3.

[84] Indeed, the legislation transposing the amended e-Privacy Directive in France permits the manifestation of consent through acceptance of default browser settings. *See* Gabriel Voisin, French Parliament publishes legislation on cookies and data breach notification, IAPP Daily Dashboard, August 26, 2011, https://www.privacyassociation.org/publications/french_parliament_publishes_legislation_on_cookies_and_data_breach_notifica.

[85] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertising, June 22, 2010, WP 171, 00909/10/EN, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf; *also see* Letter from

does not sufficiently allow individuals the ability to exercise choice on whether to share their information with third party advertisers and ad intermediaries. It conceded that once a user opts-in, separate consent is not need every time she visits a website participating in a given ad network; however, it added that separate consent must be obtained periodically and that users must benefit from an opportunity to easily revoke their consent. With respect to the reference to browser settings in Recital 66, the Working Party stated that browser settings can only suffice as an indication of user consent where the browser default is set to *reject* third party cookies (*i.e.*, the user has to actively change the browser settings to opt-in to cookie receipt); it is impossible to bypass user settings; and the browser does not allow general acceptance of all cookies, including those which may be used in the future, given that non-specific statements about cookies imply consent is uninformed.

This strict interpretation to the relationship of Article 5(3) and Recital 66 of the e-Privacy Directive was recently echoed in an opinion issued by the United Kingdom government in response to a public consultation.[86] While agreeing that "stakeholders have serious concerns around the implementation of the amended provision and that any legislative changes around the use of cookies could have serious impacts on the use of the internet", the government concluded that "[m]any respondents were clear that browser settings (though not in their current form) might be the most cost effective and efficient means of harvesting the consent of the user. However, it is the opinion of the Government that given the substantive changes to the wording of the Directive, the current use of browser setting as a form of consent is not consistent with the revised wording."[87] The Information Commissioner's Office, the United Kingdom's privacy regulator, similarly rejected the inference of consent from browser defaults.[88] EuroPriSe, the European Privacy Seal, likewise stated: "Even if the default settings of a browser were designed to reject all cookies and if then the user changed the settings to the effect that cookies should be generally accepted, one could not assume the existence of a valid informed consent. Although the modification of the browser settings could be deemed to be an indication

---

Article 29 Working Party to the Interactive Advertising Bureau (IAB) and European Advertising Standards Alliance (EASA), August 3, 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf, stating browser settings are an insufficient method to deliver meaningful consent unless they are set to reject cookies by default.

[86] United Kingdom Department for Culture, Media and Sport, Implementing the revised EU Electronic Communications Framework, HMG response to its consultation on proposals and overall approach including its consultation on specific issues, April 2011, http://www.dcms.gov.uk/images/publications/FWR_implementation_Governmentresponse.pdf.

[87] Ibid, at section 321.

[88] ICO Guidance, *supra* note 76, at p. 5. This includes use of cookies for measurement or analytics: "An analytic cookie might not appear to be as intrusive as others that might track a user across multiple sites but you still need consent." Ibid.

of wishes, this indication would neither be made in respect of the individual case – in which a cookie is stored/accessed – nor in full knowledge of all relevant facts."[89]

In the next few months, each European Union Member State will need to determine the type of permissible cookie consent as it transposes the amendments to the e-Privacy Directive into its national law.[90] Considering the wording of Article 5(3) as well as its interpretation by the Article 29 Working Party, it becomes clear that on the one hand, compliance with the amended e-Privacy Directive may only be reached if considerable adjustments are made to existing online behavioral tracking systems; while on the other hand, no "best practice" approach for the implementation of opt-in mechanisms has been identified and at the time of writing this article, no one is foreseen.

4.2. United States

While tangentially subject to various laws, such as the torts of intrusion on seclusion and public disclosure of private facts,[91] wiretapping legislation,[92] or the Computer Fraud and Abuse Act,[93] online behavioral tracking remains largely unregulated in the United States.[94] Nevertheless, the FTC has asserted itself as a strong watchdog in this domain based on its broad authority to regulate "unfair and deceptive trade practices" pursuant to Section 5 of the Federal Trade Commission Act.[95] In doing so, the FTC relied on a "notice and choice" model, whereby companies operating online are required to post detailed privacy policies describing their information collection and use practices to users, enabling users to make informed choices. Failure to adhere to one's obligations under a privacy policy could constitute a "deceptive trade practice" actionable by the FTC.[96]

---

[89] EuroPriSe, Position paper on the impact of the new "Cookie Law" on certifiability of behavioral advertising systems according to EuroPriSe, July 2010, https://www.european-privacy-seal.eu/results/Position-Papers/PDF%20-%20EuroPriSe%20position%20paper%20on%20the%20new%20cookie%20law.pdf.

[90] Several Member States have already transposed the amended Directive. *See*, *e.g.*, Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques (in France). For useful chart summarizing the implementation process see Bird & Bird, Cookies: Implementation of the new Directive, July 27, 2011, http://www.twobirds.com/English/News/Articles/Documents/BB_Privacy%20Directive%20_0711.pdf.

[91] Restatement (Second) of Torts §§ 652B, 652D (1977).

[92] Title II of the Electronic Communications Privacy Act.

[93] 18 U.S.C. § 1030.

[94] For lawsuits based on these statutes (both of which failed), *see* In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 13 (1st Cir. 2003).

[95] 15 U.S.C. § 45(a) (2006).

[96] For FTC enforcement actions based on alleged violation of self-drafted privacy policies, *see* In re Sears Holdings Mgmt. Corp., No. C-4264 (Aug. 31, 2009), http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf; FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000), available at http://www.ftc.gov/os/2000/07/toysmartconsent.htm; *also see*

However, as the FTC itself stated in its recent Preliminary Staff Report, Protecting Consumer Privacy in an Era of Rapid Change (the "Preliminary Report"): "the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[97] This view is echoed in the Department of Commerce "Green Paper" on Privacy and Innovation in the Internet Economy: "From the consumer perspective, the current system of notice-and-choice does not appear to provide adequately transparent descriptions of personal data use, which may leave consumers with doubts (or even misunderstandings) about how companies handle personal data and inhibit their exercise of informed choices."[98]

The problem with notice and choice starts with lack of transparency. Privacy policies are long documents drafted in dense legalese and read more as liability disclaimers than protection of user rights. Users do not read privacy policies, even if they are truncated and relatively interactive; simply (and quite literally) stated, life is too short for this.[99] Aleecia McDonald and Lorrie Cranor found that it would take the average user 40 minutes per day to read through all of the privacy policies she encounters online. This translates to 244 hours per year or, assuming 8 hours of sleep, 15 full days; over a lifespan of 80 years, this would mean 1,200 days, or more than 3 years life's worth of reading privacy policies. The upshot is lack of transparency into actual privacy practices and consequent diminished ability of users to make informed choices.

4.3. Self-regulation

Partly due to sparse legislation and partly a deliberate policy choice, the FTC has over the years promoted industry self-regulation in the field of online behavioral tracking. Among other initiatives, the FTC encouraged self-regulatory efforts designed to benefit users; improvements in privacy-enhancing technologies (PETs); and the creation of online privacy certification programs. However, in its recent Preliminary Report, the FTC asserted that "efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."[100]

Yan Fang, The Death of the Privacy Policy?: Effective Privacy Disclosures After In Re Sears, 25 Berk. Tech. L. J. 671 (2010).

[97] Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[98] The Department of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, December 2010, http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf, at p. 22.

[99] Aleecia McDonald & Lorrie Cranor, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review issue, http://www.casos.cs.cmu.edu/publications/papers/CostReadingPrivacyPolicies.pdf, at p. 17-18.

[100] Preliminary Report, *supra* note 97, at p. iii.

In February 2009, the FTC issued a set of self-regulatory principles to guide companies that engage in behavioral advertising.[101] These principles include: (1) transparency and consumer control (requiring websites that collect personal data to state that they are doing so and allow users to opt-out of collection); (2) reasonable security (commensurate with data sensitivity and the nature of the company's business operations); (3) limited retention for consumer data (companies may retain data only as long as is necessary to fulfill a "legitimate business or law enforcement need"); (4) affirmative express consent prior to using data in a manner materially different from promises made when the data were collected (protecting users from unexpected changes in the way their information is handled); and (5) affirmative express consent for the use of sensitive data (opt-in consent is required for the *use* of data, not for their *collection*).

This FTC's OBA Report prompted industry to launch a number of self-regulatory initiatives, including the development of new codes of conduct and online tools to allow users more control over their exposure to targeted advertising.

Indeed, the Network Advertising Initiative (NAI) updated its "Self-Regulatory Code of Conduct" in December 2008, three months prior to the release of the FTC's OBA Report.[102] In July 2009, the Interactive Advertising Bureau (IAB), together with several additional ad industry bodies, released a "Self-Regulatory Program for Online Behavioral Advertising" intended to correspond with the principles laid out by the FTC, and advocating "enhanced notice" to consumers achieved by placing a special icon on or near targeted ads.[103] The escalating debate in Europe ahead of the imminent implementation of Article 5(3) of the e-Privacy Directive induced industry organizations in this part of the world to enter the fray with their own self-regulatory proposal. In April 2011, the European Advertising Standards Alliance (EASA), a Brussels based NGO bringing together national advertising self-regulatory organizations and organizations representing the advertising industry in Europe, submitted its own best practice

[101] Federal Trade Commission, Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, February 2009, http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf ("OBA Report").

[102] Network Advertising Initiative, 2008 NAI Principles, The Network Advertising Initiative's Self-Regulatory Code of Conduct, December 2008, http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

[103] Interactive Advertising Bureau, Self-Regulatory Principles for Online Behavioral Advertising, July 2009, http://www.iab.net/media/file/ven-principles-07-01-09.pdf, stating: "Links to consumer notices will be clear, prominent, and conveniently located. This enhanced notice will be provided at the Web sites from which data is collected. Such enhanced notice will be provided at the time of such collection and use, through common wording and a link/icon that consumers will come to recognize. The opportunity for Web site users to exercise choices about whether Web viewing data can be collected and used for online behavioral advertising will never be more than a few clicks away from such standardized wording and link/icon." (Ibid, at p. 5). For review and critique of these proposals *see* Center for Democracy and Technology, Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But Still Insufficient on its Own to Protect Consumers, December 2009, http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf.

recommendation on online behavioral advertising.[104] In addition, EuroPriSe, the European privacy seal, drafted a position paper on the impact of amended Article 5(3) on the certifiability of behavioral advertising systems under its program.[105]

The NAI and IAB initiatives, while accepting the principles set forth by the FTC, restrict the scope of online behavioral tracking subject to the principles to exclude certain activities, such as "Multi-Site Advertising" and "Ad Delivery & Reporting" (NAI);[106] do not apply to third parties collecting data from websites with which they are affiliated (IAB);[107] draw a clear distinction between personally identified and non-personally identified information (both);[108] define "sensitive data" narrowly (IAB);[109] do not require affirmative opt-in consent for midstream

[104] EASA Best Practice Recommendation on Online Behavioral Advertising, April 2011, http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011.pdf/download.

[105] EuroPriSe, *supra* note 89, at p. 13-14.

[106] According to the NAI Principles, "Multi-Site Advertising" means ad delivery and reporting across multiple domains owned or operated by different entities; whereas "Online Behavioral Advertising" means any process used whereby data are collected across multiple domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online. The CDT states that "while the NAI has extended nearly all of its principles (i.e., notice, transfer and service restrictions, access, reliable sources, security, and data retention) to cover Online Behavioral Advertising and Multi-Site Advertising, the NAI has neither established a choice requirement for Multi-Site Advertising nor specifically applied its use limitations principle to Multi-Site Advertising." Center for Democracy and Technology, Online Behavioral Advertising: Industry's Current Self-Regulatory Framework Is Necessary, But Still Insufficient On Its Own To Protect Consumers, Dec. 9, 2009, http://www.cdt.org/policy/online-behavioral-advertising-industry%E2%80%99s-current-self-regulatory-framework-necessary-still-in.

[107] Consider that the "Google family" of companies is present on circa 60% of all websites (as of September 2008); *see* Krishnamurthy & Wills, *supra* note 46.

[108] The distinction between personally identified information (PII) and non-PII becomes murky given the increased amounts of data stored and enhance analytics abilities, the combination of which allows re-identification of *see*mingly anonymized data sets. For example, online behavioral tracking companies may collect anonymous data but then overlay it with other databases, in an attempt to bring users' identity into clearer focus. Paul Ohm recently observed : "Clever adversaries can often re-identify or de-anonymize the people hidden in an anonymized database… Re-identification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization. "Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010). De-anonymization of *see*mingly anonymous databases was recently demonstrated by researchers who were able to identify a large proportion of anonymized Netflix subscribers by matching data in their movie ratings against an additional online database. Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy 111. In another case, two New York Times reporters were able to sparse out the identity of an AOL user, whose online search queries were anonymized and posted on an AOL research website. Michael Barbaro & Tom Zeller, A Face is Exposed for AOL Searcher No. 4417749, NY Times, Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html. The seminal research in this respect dates back to 2000: Latanya Sweeney, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy Working Paper, LIDAP-WP4 (2000) (demonstrating that merely three pieces of information – ZIP code, birth date, and gender – are sufficient to uniquely identify 87% of the United States population).

[109] The IAB Principles define "sensitive data" as "financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual". IAB Principles, *supra* note 103, at p. 40. This definition omits additional categories of data typically considered to be sensitive, such

changes in privacy policies (NAI);[110] and divorce the principle of limited retention from that of purpose specification, thus permitting retention for unspecified secondary business purposes (both).[111]

The EASA best practice recommendations in Europe are based on five principles: (1) notice, including "enhanced notice" through use of an icon linked to comprehensive background information and control mechanisms; (2) choice, providing users with a one-stop-shop solution for opting-out of online behavioral tracking,[112] and requiring explicit consent for collecting data about all or substantially all websites a user visited;[113] (3) sensitive data, avoiding targeting of children or tracking based on sensitive categories of data;[114] (4) compliance and enforcement programs, requiring effective mechanisms be put in place to ensure compliance and complaint handling; and (5) review, subjecting the recommendations to periodic review and modification. These recommendations were criticized by the World Privacy Forum, an advocacy group, for not invoking privacy as a policy goal, instead citing "consumer transparency and choice".[115] The World Privacy Forum argued that the distinction drawn by EASA between "online behavioral advertising" (which is covered by the recommendations) and "ad reporting" and "ad delivery" (which are not covered) overly restricts the scope of the recommendations and omits multi-site tracking which significantly impacts user privacy. In addition, the recommendations are limited to the online sphere, whereas much of the tracking has now shifted to other platforms, such as mobile phones and video game consoles. Moreover, the World Privacy Forum advocates a shift from a binary approach based on whether or not a user has given consent to online behavioral

---

as information about an individual's intimate relations or sexual orientation; financial information; or, increasingly, location data. *See*, e.g., Electronic Frontier Foundation, On Locational Privacy, and How to Avoid Losing it Forever, August 2009, http://www.eff.org/files/eff-locational-privacy.pdf; Article 29 Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, WP115, Nov. 25, 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

[110] The FTC guidelines state that "before a company can use previously collected data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers." The NAI version is far more restrictive: "If a member changes its own privacy policy with regard to PII and merger with non-PII for OBA, prior notice shall be posted on its website."

[111] This, of course, is not coincidental and reflects a fundamental policy choice regarding the intersection of three important data protection principles: purpose limitation, data minimization, and retention limitation. *See* discussion in CDT, Online Behavioral Advertising, *supra* note 103, at p. 30.

[112] *See* http://www.youronlinechoices.eu.

[113] *See supra* notes 43-**Error! Bookmark not defined.** and accompanying text.

[114] While the EASA Best Practice Recommendations do not define "sensitive data", the IAB Europe EU Framework for Online Behavioral Advertising, attached thereto, does: "sensitive personal data as defined under Article 8.1 of Directive 95/46/EC". This, in turn, is a rather broad definition including "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".

[115] The World Privacy Forum, Comments on EASA Best Practice Recommendation on Online Behavioral Advertising, Feb. 25, 2011, http://www.worldprivacyforum.org/pdf/WPF_EASA_comment_2011fs.pdf.

tracking to one requiring online parties to implement privacy by design even where processing is authorized by the user.[116]

At this point in time, it appears that self-regulation has yet to be successful in relaxing consumers' concerns about privacy, fulfilling businesses' interest in clarity, and satisfying regulators' calls for additional enforcement tools.[117] Referring to the OBA Report, the FTC states: "This report prompted industry to launch a number of self-regulatory initiatives, including the development of new codes of conduct and online tools to allow consumers more control over the receipt of targeted advertising… [T]hese efforts have not yet been fully implemented and their effectiveness has yet to be demonstrated".[118] This is also the view of the Department of Commerce: "This Green Paper illustrates the power of applying cooperative, multi stakeholder principles. But in certain circumstances, we recognize more than self-regulation is needed."[119] Indeed, one of the main developments called for in the Department of Commerce Green Paper is the establishment of a Privacy Policy Office in the Executive Branch, which would act as a convener of diverse stakeholders and work with the FTC to lead efforts to develop voluntary, enforceable codes of conduct.[120] To incentivize online businesses to join the self-regulatory bandwagon, the Green Paper suggests creating a safe harbor against FTC enforcement for companies that commit and adhere to an appropriate code of conduct.[121]

5. Proposals for regulatory reform

The past year featured a burst of activity in Washington focused on both online and offline privacy regulatory reform. It has been anchored by the FTC Preliminary Report, followed by a swift response from industry, and reinvigorated by a slew of legislative bills. It included the creation for the first time of a dedicated Senate Sub-Committee on Privacy, Technology and the Law, headed by Senator Al Franken (D-MN) and charged with "oversight of laws and policies

[116] Additional criticism is pointed at the EASA recommended compliance and enforcement mechanism. *See* ibid, at p. 9-13.

[117] Wired magazine noted in August 2009 that attempts at self-regulation by the online behavioral tracking and advertising industry "have conspicuously failed to make the industry transparent about when, how
and why it collects data about internet users." Ryan Singel, You Deleted Your Cookies? Think Again, Wired, Aug. 10, 2009, http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again.

[118] FTC Report, at p. 15.

[119] Green Paper, at p. iv.

[120] Ibid, at p. 5-6, 45-50.

[121] Ibid, at p. 43. Further clarifying that "the 'carrot' offered by a safe harbor has force only if there is a corresponding 'stick.' That is, a safe harbor is only as effective as the perceived threat of legislative, regulatory, or other legal risk faced by the company in absence of the ability to resort to safe harbor protection."

governing the collection, protection, use, and dissemination of commercial information by the private sector, including online behavioral advertising."[122]

5.1. The FTC Do Not Track Proposal

The FTC Preliminary Report sets forth three central axes for future regulation of online privacy: First, privacy by design, according to which companies should promote privacy protections throughout the organization and at every stage of the development of products and services starting at the design phase; such protections should include providing data security; collecting only those data that are required for a specific business purpose (data minimization); retaining data only long enough to fulfill that purpose (retention limitation); and ensuring reasonable data accuracy (data quality).[123]

Second, simplified choice, meaning that on the one hand, companies need not provide choice before collecting and using data for "commonly accepted" practices such as product fulfillment, internal operations, fraud prevention, legal compliance, and first-party marketing; on the other hand, for practices requiring choice, companies must offer choice at a time and in a context in which the user is making a decision about her data, and implement a DNT mechanism for online behavioral advertising.

Third, increased transparency, calling for privacy notices to be clearer, shorter, and more standardized; for companies to provide reasonable access to any data they maintain, in proportion to the sensitivity of the data and the nature of their use; and for companies to provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different from that presented at the time of collection.[124]

Most of the public debate following the FTC's Preliminary Report focused on the DNT proposal for compliance with a user's centralized opt-out of online behavioral tracking. The FTC contemplates that DNT could be advanced by either legislation or enforceable industry self-regulation.[125] It states that "[t]he most practical method of providing uniform choice for online

---

[122] http://www.judiciary.senate.gov/about/subcommittees/privacytechnology.cfm.

[123] Kashmir Hill, Why 'Privacy By Design' is the New Corporate Hotness, Forbes, July 27, 2011, http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness.

[124] In statements recently made to the Technology Policy Institute's Aspen Forum, FTC Commissioner J. Thomas Rosch recently emphasized transparency, rather than user choice, as the key aspect of DNT. *See* Declan McCullagh, FTC commissioner calls for new 'do not track' approach, CNet, August 22, 2011, http://news.cnet.com/8301-31921_3-20095536-281/ftc-commissioner-calls-for-new-do-not-track-approach/#ixzz1WViQTVQx.

[125] On February 11, 2011, Representative Jackie Speier (D-CA) introduced the Do Not Track Me Online Act of 2011, H.R. 654, which would direct the FTC to promulgate DNT regulation for the use of "an online opt-out mechanism to allow a consumer to effectively and easily prohibit the collection or use" of online activity and "to require a covered entity to respect the choice of such consumer to opt-out of such

behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices."[126] In addition, the FTC stresses that DNT differs from Do Not Call in that it will not necessitate a central registry, instead relying on a browser-based mechanism through which users could make persistent choices.[127]

Even before implementing DNT, most online behavioral tracking companies offer end users the option to opt-out of tracking cookies. Such an opt-out typically relied on the users clicking to accept an opt-out cookie. However, opt-out cookies were often deleted when users cleared their cookie folder, tossing such users unknowingly back into the ad targeting pool. In addition, the lack of a well-known central location for opting-out required users to review privacy policies in order to discover links to opt-out tools. Finally, the FTC noted: "existing mechanisms may not make clear the scope of the choices being offered. It may not be clear whether these mechanisms allow consumers to choose not to be tracked, or to be tracked but not delivered targeted advertising." Hence, a robust DNT mechanism must clarify to users not only *how* they can exercise their opt-out right but also *what* exactly they are opting-out of? Is it data collection or only ad targeting? And what exactly does "tracking" mean in this context?

5.2. Industry proposals

Before drawing FTC support, DNT was an advocacy group initiative, submitted during an FTC workshop on behavioral advertising in October 2007. The privacy group proposed: "To help ensure that [the privacy principles] are followed, the FTC should create a national DNT List similar to the national Do Not Call List."[128] The proposal would have required advertisers to

---

collection or use". Under the bill, businesses would be required to disclose their information practices to users in an "easily accessible" manner.§3.
http://speier.house.gov/uploads/Do%20Not%20Track%20Me%20Online%20Act.pdf. On May 6, 2011, Representatives Ed Markey (D-MA) and Joe Barton (R-TX) introduced the Do Not Track Kids Act of 2011, amending the Children's Online Privacy Protection Act of 1998 (COPPA) to prevent online behavioral tracking of children as well as teens under 18. On May 9, 2011, Senator Jay Rockefeller (D-WV) introduced the "Do-Not-Track Online Act of 2011", which would instruct the FTC to promulgate regulations that would create standards for the implementation of a DNT mechanism and prohibit online service providers from tracking individuals who use DNT to opt-out. The regulations would allow online service providers to track individuals who opt-out only if tracking is necessary to provide a service requested by the individual and the individuals' information is anonymized or deleted when the service is provided; or the individual is given clear notice about the tracking and affirmatively consents.

[126] FTC Preliminary Report, at p. 66.

[127] Ibid, at p. 67.

[128] Ari Schwartz, Deputy Director Center for Democracy and Technology, Linda Sherry, Director, National Priorities Consumer Action, Mark Cooper, Director of Research Consumer Federation of America, et al, Consumer Rights and Protections in the Behavioral Advertising Sector, submitted in advance of the FTC

submit their tracking domains to the FTC, which would make a DNT list available on its website for download by users who wish to limit tracking. The idea remained dormant until July 2009, when privacy advocate Christopher Soghoian first developed his Targeted Advertising Cookie Opt-Out (TACO) mechanism as a prototype plug-in that automatically checks for a header on a website to determine whether to allow tracking cookies.[129] Version 3.0 of the TACO plug-in could block a total of 95 advertising networks; show granular detail on which tracking systems a website was using; and display them on a console when a user visits a new web page. Further controls allowed users to block particular tracking systems while allowing others. But the concept failed to resonate with the broader policy or advertising communities. Soghoian and his research collaborator Sid Stamm later put together a prototype Firefox add-on that added a DNT header to outgoing HTTP requests, which is the precursor to the headers that are being implemented by industry today.

DNT first gained momentum as a viable policy concept in July 27, 2010, when FTC Chairman Jon Leibowitz testified at the Senate Committee on Commerce, Science and Transportation on efforts to protect consumer privacy.[130] Departing from scripted remarks, Chairman Leibowitz stated that the FTC is calling for an industry-led DNT program. Stanford researchers Jonathan Mayer and Arvind Narayanan followed suit by creating "donottrack.us" to provide "a web tracking opt-out that is user friendly, effective, and completely interoperable with the existing web." Their approach, like Soghoian and Stamm's before them, depends on internet browsers sending a header to permit the placement of tracking cookies on a user's computer. "Unlike Do Not Call, DNT is not a list; rather, it employs a decentralized design, avoiding the substantial technical and privacy challenges inherent to compiling, updating, and sharing a comprehensive registry of tracking services or web users."[131]

Initial industry response was hardly enthusiastic, declaring that "[i]f mandated by the government, this would be tantamount to a government-sponsored, and possibly managed, ad-blocking program – something inimical to the First Amendment".[132] DNT was seen as distraction from self-regulatory efforts organized by advertising industry groups, which were based on icons on behavioral ads leading to opt-out tools. However, the release of the FTC's Preliminary Report in December 2010 prompted the major browser makers to engage with the DNT proposal.

Town Hall, Ehavioral Advertising: Tracking, Targeting, and Technology, Nov 1-2, 2007, http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf.

[129] Christopher Soghoian, TACO 2.0 released, slight paranoia blog, July 27, 2009, http://paranoia.dubfire.net/2009/07/taco-20-released.html; Jeremy Kirk, Privacy Add-ons Merged to Create Powerful Tool, PC World, June 15, 2010, http://www.pcworld.com/businesscenter/article/198852/privacy_addons_merged_to_create_powerful_tool.html. *Also see* Christopher Soghoian, The History of the Do Not Track Header, slight paranoia blog, Jan. 21, 2011, http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

[130] Prepared Statement of the Federal Trade Commission on Consumer Privacy, Presented By Chairman Jon Leibowitz Before the Committee on Commerce, Science, and Transportation, United States Senate, July 27, 2010, http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

[131] Do Not Track: Universal Web Tracking Opt-Out, http://donottrack.us.

[132] IAB Reviews Preliminary FTC Staff Report on Protecting Consumer Privacy, Dec. 1, 2010, http://www.iab.net/public_policy/1481209.

In December 2010, Microsoft implemented a "Tracking Protection" feature in its new Internet Explorer 9 browser, allowing users to select a Tracking Protection List (TPL) from a choice provided by various organizations, such as Abine, EasyList, PrivacyChoice, and TRUSTe.[133] Simply stated, a TPL contains web addresses that the browser will visit only if a user typed in their address or linked to them directly. Indirect access to a listed website is blocked, so if a web page contains links to other content from blocked addresses, such links are not visited and cookies from such website are blocked. Microsoft states that the new feature "provid[es] a new browser mechanism for consumers to opt-in and exercise more control over their browsing information. By default the Tracking Protection List is empty, and the browser operates just as it does today." While presented as an opt-in mechanism, TPL is really an opt-out tool (which users may choose to opt-into).[134] Despite earlier skepticism about the concept, Microsoft also added a DNT browser header, which is automatically activated when a TPL (even an empty one) is uploaded, in its final release of Internet Explorer 9.[135]

Mozilla, maker of the Firefox browser, presented an approach based on a DNT browser header. On January 23, 2011, Mozilla released Firefox 4, which allows users to check a "Do Not Track" box in the "advanced" settings of the browser, prompting a header to be sent with every click or page request signaling to websites that the user does not wish to be tracked.[136] Unlike Microsoft's TPL solution, the DNT header leaves it entirely up to receiving websites to honor the user's request by omitting any tracking cookies from their response. As the CDT explains, "Firefox users will have to rely upon individual websites to honor their 'Do Not Track' requests. Today, websites do not have the infrastructure to accommodate these requests (…)"[137]

Google, maker of the Chrome browser, took a different approach, introducing the Keep My Opt-Outs plug-in, allowing users to permanently opt-out of online behavioral tracking by companies participating in self-regulatory programs.[138] The new plug-in was meant to remedy the recurrent problem whereby users cleared out any opt-out cookies when purging their cookie folder, thus unknowingly re-entering the tracking domain. Keep My Opt-Outs is itself cookie based; deleting all cookies sent by registered domains and adding a DNT cookie for such domains.

---

[133] IE9 and Privacy: Introducing Tracking Protection, IE Blog, Dec. 7, 2010, http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx. To activate TPL, users are directed from the browser's "safety" tab to a web page featuring lists of tracking companies compiled by various organizations. DNT is automatically enabled once a user selects a tracking list.

[134] Microsoft purportedly shelved a similar feature several years ago, under intense pressure from online advertisers. Nick Wingfield & Julia Angwin, Microsoft Adds Do-Not-Track Tool to Browser, Mar. 15, 2011, http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html.

[135] Ibid.

[136] Privacy/Jan2011 DoNotTrack FAQ, Mozilla Wiki, Jan. 24, 2011, https://wiki.mozilla.org/Privacy/Jan2011_DoNotTrack_FAQ.

[137] Aaron Brauer-Rieke, "Do Not Track" Gains Momentum as Mozilla Announces New Tracking Tool, CDT Blog, Jan. 24, 2011, http://www.cdt.org/blogs/aaron-brauer-rieke/%E2%80%9Cdo-not-track%E2%80%9D-gains-momentum-mozilla-announces-new-tracking-tool.

[138] Sean Harvey & Rajas Moonka, Keep Your Opt-outs, Jan. 24, 2011, http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

Apple too added a DNT tool to a test version of its Safari browser included within the latest version of Lion, its new operating system currently available only to developers.[139]

Each of the industry mechanisms for implementation of DNT has its own costs and benefits.[140] The FTC put forth the following criteria to assess industry responses: DNT should be universal, that is, a single opt-out should cover all would-be trackers; easy to find, understand, and use; persistent, meaning that opt-out choices do not "vanish"; effective and enforceable, covering all tracking technologies; and controlling not only use of data but also their collection.[141] As discussed, the FTC has not yet taken a position on whether any legislation or rulemaking is necessary for DNT. It is clear, however, that regardless of the regulatory approach chosen, industry collaboration will remain key since the system will only work if websites and ad intermediaries respect users' preferences.

5.3. Draft Legislation

The renewed public interest in privacy and online behavioral tracking, spurred by the Wall Street Journal "What They Know" series,[142] FTC and Department of Commerce engagement with the topic, and occasional front-page privacy snafu (*e.g.*, Google Buzz,[143] iPhone location tracking[144]), have led to an unprecedented flurry of activity and legislative proposals on the Hill.[145] All bills address transparency and choice requirements, and several refer specifically to DNT.

---

[139] Nick Wingfield, Apple Adds Do-Not-Track Tool to New Browser, Wall Street Journal, Apr. 14, 2011, http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html. For a proposal of implementing DNT through client – as opposed to server-side solutions, see Mikhail Bilenko, Matthew Richardson, and Janice Tsai, Targeted, Not Tracked: Client-side Solutions for Privacy-Friendly Behavioral Advertising, Privacy Enhancing Technologies Symposium 2011, http://petsymposium.org/2011/papers/hotpets11-final3Bilenko.pdf.

[140] For a comparison of proposed mechanisms *see* Alissa Cooper & Hannes Tschofenig, Overview of Universal Opt-Out Mechanisms for Web Tracking, Mar. 7, 2011, http://tools.ietf.org/html/draft-cooper-web-tracking-opt-outs-00#page-12; Comments of Jim Brock, Founder and CEO, PrivacyChoice LLC, submitted to the FTC in response to the Preliminary Report, http://www.ftc.gov/os/comments/privacyreportframework/00455-57999.pdf. The EFF views Mozilla's browser header as the best solution, stating "Mozilla is now taking a clear lead and building a practical way forward for people who want privacy when they browse the web." Rainey Reitman, Mozilla Leads the Way on Do Not Track, EFF Blog, Jan. 24, 2011, https://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track.

[141] Ed Felten, FTC Perspective, W3C Workshop on Web Tracking and User Privacy, Apr. 28-29, 2011, http://www.w3.org/2011/track-privacy/slides/Felten.pdf.

[142] http://online.wsj.com/public/page/what-they-know-digital-privacy.html.

[143] Amir Efrati, Google Settles Privacy Lawsuit for $8.5 Million, Wall Street Journal, Sept. 3, 2010, http://online.wsj.com/article/SB10001424052748703946504575470510382073060.html; Julia Angwin& Amir Efrati, Google Settles With FTC Over Google Buzz, Wall Street Journal, Mar. 31, 2011, http://online.wsj.com/article/SB10001424052748703806304576232600483636490.html.

[144] Alasdair Allan &Pete Warden, Got an iPhone or 3G iPad? Apple is recording your moves, O'Reilley Radar, Apr. 20, 2011, http://radar.oreilly.com/2011/04/apple-location-tracking.html.

[145] In addition to the comprehensive legislation outlined below, two bills were submitted dealing with DNT and one with online behavioral tracking of children. *See* discussion text for *supra* note 125.

The BEST PRACTICES Act. On July 19, 2010, House Representative Bobby Rush (D-IL) introduced a privacy bill,[146] which would establish national requirements for collecting and sharing personal information, codifying certain fair information principles into law. The bill mandates increased transparency, requiring covered entities to make specific privacy disclosures to individuals whose personal information they collect or retain "in concise, meaningful, timely, prominent, and easy-to-understand" fashion, with a special provision allowing the FTC to introduce standardized short-form notices that users are more likely to understand.[147] It requires that mechanisms be put in place to facilitate user choice, providing users with a "reasonable means" to opt-out of information collection and use for non-operational purposes;[148] however, businesses may explicitly condition a service on a user not opting-out of secondary usage.[149] The bill requires opt-in consent for (a) the collection, use or disclosure of sensitive information, which includes medical history, race, ethnicity or religious beliefs, sexual orientation or sexual behavior, financial information, precise geolocation information, and biometric data;[150] (b) disclosure of covered information to third parties for non-operational purposes;[151] (c) any "material" changes to privacy practices governing previously collected information;[152] and (d) use of software or hardware to monitor all or substantially all of an individual's browsing activity.[153]

To promote enforceable industry self-regulation, the bill would provide a "safe harbor" substituting opt-in consent requirements for opt-outs, where companies enroll in FTC-monitored and approved universal opt-out programs operated by industry self-regulatory programs ("Choice Programs").[154] Choice Programs would, at minimum, would be required to (a) provide a clear and conspicuous opt-out mechanism from third party information sharing; (b) provide users with a clear and conspicuous mechanism to set communication, online behavioral advertising, and other preferences that will apply to all covered entities participating in a Choice Program; and (c) establish procedures for testing and review of Choice Program applications, periodic assessment of members, and enforcement for violations by participating entities.[155]

While not expressly endorsing DNT, the bill does not exclude it as a means to obtain user consent.[156]

---

[146] H.R. 5777; 111th Congress. On February 10, 2011, Rep. Rush re-introduced the bill in the 112th Congress as H.R. 611. *See* http://www.gpo.gov/fdsys/pkg/BILLS-112hr611ih/pdf/BILLS-112hr611ih.pdf.
[147] §102.
[148] §103(a)-(e).
[149] §103(f).
[150] §104(b).
[151] §104(a)(1).
[152] §105(a). The bill also requires covered entities to post new privacy policies that include any such material changes at least 30 days in advance of collecting information pursuant to those policies. §105(b).
[153] §104(c).
[154] §401.
[155] §§403-404.
[156] Upon re-introduction of his bill in the 112th Congress, Representative Rush said "I do not oppose DNT. In fact, in order for companies to qualify under the FTC Safe Harbor program contained in my bill, they

Commercial Privacy Bill of Rights Act of 2011. On April 12, 2011, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the Commercial Privacy Bill of Rights Act of 2011, intended to "establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the FTC." The bill directs the FTC to promulgate rules to require covered entities to provide clear, concise, timely notice of their information collection, use, transfer, and storage practices. In addition, a covered entity would be required to provide clear, concise, and timely notice to individuals before changing its practices in a material way.[157] It would not, however, be required to obtain opt-in consent to such changes; rather opt-in consent would only be necessary where a change creates risk of economic or physical harm to an individual.[158]

The bill would require a covered entity to offer individuals a clear and conspicuous opt-out mechanism for any "unauthorized use" of covered information, except for any use requiring opt-in consent.[159] "Unauthorized use" is defined as use for any purpose "not authorized by the individual;" except certain "commonly accepted" uses by a covered entity or its service provider; including first-party marketing, analytics and ad-tracking; so long as the covered information used was either collected directly by the covered entity or by its service provider.[160] A "robust, clear, and conspicuous mechanism for opt-out consent" must also be provided for the use by third parties of the individuals' covered information for behavioral advertising or marketing.[161] Opt-in rights must be provided under the bill for collection, use, or transfer of sensitive

---

would have to set up a 'DNT like' mechanism for consumers to allow them to opt-out of having the personal information they provide, both online and offline, to third parties." Rep. Bobby Rush, Press Release, Feb. 11, 2011, http://www.house.gov/apps/list/press/il01_rush/pr_110211_hr611.shtml.

[157] §201.

[158] §202(a)(3)(B).

[159] §202.

[160] §3(8). In the context of online behavioral tracking, it is worth noting the following exceptions from the definition of "unauthorized use" (meaning that the following activities *do not* require opt-out rights): "To market or advertise to an individual from a covered entity within the context of a covered entity's own Internet website, services, or products if the covered information used for such marketing or advertising was - (I) collected directly by the covered entity; or (II) shared with the covered entity (aa) at the affirmative request of the individual; or (bb) by an entity with which the individual has an established business relationship." (§3(8)(B)(vi)). "Use that is necessary for the improvement of transaction or service delivery through research, testing, analysis, and development." (§3(8)(B)(vii)). "Use that is necessary for internal operations, including the following: (…) Information collected by an Internet website about the visits to such website and the click-through rates at such website—(aa) to improve website navigation and performance; or (bb) to understand and improve a the interaction of an individual with the advertising of a covered entity." (§3(8)(B)(viii)(II)). "Use— (I) by a covered entity with which an individual has an established business relationship; (II) which the individual could have reasonably expected, at the time such relationship was established, was related to a service provided pursuant to such relationship; and (III) which does not constitute a material change in use or practice from what could have reasonably been expected." (§3(8)(B)(ix)).

[161] §202(a)(2). A "third party" is defined as a person that is not related to the covered entity by common ownership or control; is not the covered entity's service provider; does not have an "established business relationship" with the individual; and does not identify itself to the individual at the time of information collection. The term ''established business relationship'' means a relationship formed with or without consideration, involving the establishment of an account for the receipt of products or services. §3(4).

information, except in limited circumstances; as well as for the use or transfer to a third party of previously collected covered information for an unauthorized use or where there is a material change in the covered entity's stated practices and the use or transfer creates a risk of economic or physical harm to an individual.[162]

The bill directs the FTC to issue rules to establish safe harbor "co-regulatory programs" to be administered by non-governmental organizations.[163] The programs would establish mechanisms for participants to implement the bill's requirements with regard to online behavioral advertising, location-based advertising, and other unauthorized uses.[164] The programs would offer consumers a clear, conspicuous, persistent, and effective means of opting-out of the transfer of covered information by a participant in the safe harbor program to a third party.[165]

Consumer Privacy Protection Act of 2011. The Rush bill contains a number of provisions similar to a discussion draft of privacy legislation, which was published by Representatives Rick Boucher (D-VA) and Cliff Stearns (R-FL) in May 2010.[166] On April 13, 2011, Rep. Stearns formally introduced a revised version of the measure, co-sponsored by Rep. Jim Matheson (D-UT),[167] as the Consumer Privacy Protection Act of 2011.[168] The bill would obligate covered entities to provide users with a privacy notice: (a) before personal information is used for a purpose unrelated to a "transaction,"[169] which is broadly defined to include "an interaction between a consumer and a covered entity resulting in any use of information that is necessary to complete the interaction in the course of which information is collected, or to maintain the provisioning of a good or service requested by the consumer, including use (…) related to website analytics methods or measurements for improving or enhancing products or services (…) and (…) the collection or use of personally identifiable information for the marketing or advertising of a covered entity's products or services to its own customers or potential customers;"[170] and (b) upon any material change in the covered entity's privacy policy.[171] Such a notice would be provided "in a clear and conspicuous manner, be prominently displayed or explicitly stated to the consumer", and state that personal information may be used or disclosed for purposes or transactions unrelated to that for which it was collected, or that there has been a material change in the covered entity's privacy policy.[172] In addition, the bill would require covered

[162] §202(a)(3).
[163] §501.
[164] Ibid.
[165] Ibid.
[166] http://www.nciss.org/legislation/BoucherStearnsprivacydiscussiondraft.pdf.
[167] Rick Boucher failed to get re-elected in the 2010 mid-term elections. Tony Romm, Tech community laments Rick Boucher loss, Politico, Nov. 2, 2010, http://www.politico.com/news/stories/1110/44589.html.
[168] H.R. 1528, http://stearns.house.gov/UploadedFiles/Privacy_Bill.pdf.
[169] §4(a)(1).
[170] §§3(15)(A)(iv); 3(15)(E).
[171] §4(a)(2).
[172] §4(b).

entities to provide users with a "brief, concise, clear, and conspicuous" "privacy policy statement" "written in plain language".[173]

Under the bill, users must be offered an opportunity to prevent at no charge for a period of up to five years (unless the user indicates otherwise,) the sale or disclosure for consideration of their personal information for a purpose other than the transaction it was collected for.[174] The provision of such an opt-out right is not required: (a) if the personal information transferee is an ''information-sharing affiliate", defined as "an affiliate that is under common control with a covered entity, or is contractually obligated to comply with" its privacy policy statement.[175] Realizing that the transfer of personal data often constitutes a primary, not secondary part of the business transaction, the bill permits a covered entity to provide a consumer an opportunity to authorize the sale or disclosure of her personal information "in exchange for a benefit to the consumer". The opportunity offered to consumers to preclude or permit the sale or disclosure for consideration of their personal information "must be both easy to access and use, and the notice of the opportunity to preclude must be clear and conspicuous".[176]

Generally speaking, the Stearns-Matheson bill would solidify the notice and choice paradigm criticized by the FTC and Department of Commerce. Unlike the Kerry-McCain and Rush bills, it does not obligate entities to obtain opt-in consent in any circumstance.

6. Moving forward

What is the right tradeoff between privacy and enhanced online functionality? The **industry** argues online behavioral tracking generates immense value, facilitates innovation and helps drive the most important revolution since the invention of print.[177] Many **privacy advocates** will continue beating the privacy risk drum regardless of the contents of notice or positioning of opt-out.[178] They will argue that users are never educated enough to make the "right" choice concerning online behavioral tracking, unless they decide to reject it altogether. Even if users

[173] §5.
[174] §6(a).
[175] §§6(a) and 3(7).
[176] §6(b).
[177] *See*, e.g., Omar Tawakol, Chief Executive Officer, BlueKai, Proposal for Browser Based Do-Not-Track Functionality, submission to W3C Workshop on Web Tracking and User Privacy, Mar. 25, 2011, http://www.w3.org/2011/track-privacy/papers/BlueKai.pdf, stating: "Without data targeting, publishers can either force users to pay, or force them to *see* the ad before the content (or both). Polls of users such as that done by MarketingSherpa have shown that overwhelmingly users (even the ones that don't like ads) prefer to get free content sponsored by targeting over having to pay for the content. Therefore, we strongly encourage the W3C to ensure that any DNT functionality provides the marketplace with the opportunity to recognize the full economic tradeoff that consumers are making when it comes to online tracking."
[178] *See*, e.g., Comments of the Center for Digital Democracy and U.S. PIRG, submitted to the FTC, Feb. 18, 2011, http://www.centerfordigitaldemocracy.org/sites/default/files/2011-02-17-FTC-Comments.pdf.

made crystal clear their indifference about targeted ads, some privacy advocates would likely argue that tracking should be restricted given the (admittedly unlikely) chance that the government may seek to seize and re-identify individual profiles. The **general public**, meanwhile, often expresses in opinion polls an interest in privacy and aversion towards online behavioral tracking.[179] Yet such results should be tempered against the reality that users consistently refrain from taking any step, no matter how trivial and costless, to prevent tracking. What does it mean to be "for privacy" or "against tracking", and at the same time unwilling to check a box or pay a single penny to preserve one's rights?[180] Many advocates will suggest that the choices are too confusing or too hard to exercise, but even when the choice is as basic as unchecking a clearly visible tick-box, the default continues to rule the day. And when users perceive a benefit, even if small, they quickly share their data.[181] Why do people express support for privacy and resistance to surveillance, yet at the same time enroll in biometric or RFID-based identification systems to save a few minutes in mass transport systems,[182] airports,[183] and banks?

This implies that a key vector in evaluating the underlying value judgments is whether it is acceptable to weigh social benefits beyond the value to an individual user. The value of data collection and use to broader society includes ease of obtaining credit, support of free web content, encouraging users to conserve energy,[184] and more. Given that individual users when asked to make a choice may decline, but when not asked will not take the initiative to decline even though there is an opportunity to do so effortlessly, the decision between opt-in or opt-out determines the fate of entire business models. If the value of a given activity to society is not significant, then the focus can be on the right of an individual to choose and the requirement that such a choice be informed. But if the societal benefit is relevant, then it may be entirely acceptable to set the default such that users are required to take an initiative to decline.

---

[179] Turow et al, *supra* note 56.

[180] *See*, e.g., Graeme McMillan, Less Than 1% of Firefox Users Use 'Do Not Track' Function, Time Techland, Apr. 25, 2011, http://techland.time.com/2011/04/25/less-than-1-of-firefox-users-use-do-not-track-function/#ixzz1LyYlg7Ma.

[181] For an in-depth discussion of the means to ascertain the "value of privacy" to individuals, *see* Alessandro Acquisti, Leslie John & George Loewenstein, What is privacy worth? Leading paper, 2010 Future of Privacy Forum's Best "Privacy Papers for Policy Makers" Competition, http://www.futureofprivacy.org/wp-content/uploads/2010/09/privacy-worth-acquisti-FPF.pdf.

[182] *See*, e.g., Gaby Hinsliff, MI5 *see*ks powers to trawl records in new terror hunt, Guardian, Mar. 16, 2008, http://www.guardian.co.uk/uk/2008/mar/16/uksecurity.terrorism, discussing access of UK security organizations to database of Oyster travel cards.

[183] *See*, e.g., Atos Origin, UK Passport Service Biometrics Enrolment Trial Report, May 2005, http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf , finding that the majority of participants felt biometrics would help with passport security, preventing identity fraud and curbing illegal immigration.

[184] *See*, e.g., Future of Privacy Forum & Ontario Information and Privacy Commissioner Ann Cavoukian, SmartPrivacy for the Smart Grid: Embedding Privacy in the Design of Electricity Conservation, November 2009, http://www.futureofprivacy.org/wp-content/uploads/2009/11/smartprivacy-for-the-smart-grid.pdf.

We think that the discussion raging around DNT proves our point. People are worked up not about the mechanics of opt-out or specifics of notice; rather they are up in arms because the simplicity of DNT crystallizes the deep ideological divide about right and wrong in cyberspace into a binary "on/off" switch. People realize fully well that whether a practice is part of DNT or not constitutes a far-reaching policy statement about such practice's social desirability. We should not lose sight of the real issue, though, and it is not whether analytics, measurement, or third party cookie sharing constitutes "tracking" or not; rather it is whether those activities carry an important social value which we wish to promote, or are negative and thus better be "killed softly".

In our opinion, the underlying value question remains open, unanswered, and far from consensus, and this will inevitably undermine efforts to resolve the online behavioral tracking debate. Without derogating from the importance and utility of discussion such as that held by the W3C Workshop on Web Tracking and User Privacy,[185] it may be premature to debate technical standardization of DNT mechanisms before making this value judgment. And the value judgment required is not one for engineers or lawyers to make. It cannot be discerned from harmonization of network protocols or etymological analysis of the words "track" or "third party". It is not a technical or legal question; it is a social, economic, even philosophical quandary.

6.1. Demystifying Consent

Personal data have become a primary feature of the value exchange in almost any online transaction. Individuals acquiring goods or consuming services online, often at no monetary cost, are also giving (or selling) something, namely, their personal information.[186] For the most part, individuals have little knowledge and understanding of the potential value of this economic exchange; do not know what will be done with the information; and do not grasp the full implications of consenting to release of information.[187] And yet the overwhelming majority of such value-for-data transactions are legally based on users' informed consent. We believe this reflects an omission on the part of policymakers to make a value judgment with respect to the social desirability of online behavioral tracking.

[185] W3C Workshop on Web Tracking and User Privacy, Apr. 28-29, 2011, Princeton, NJ, USA, http://www.w3.org/2011/track-privacy.
[186] Jeroen van den Hoven, Privacy and the Varieties of Informational Wrongdoing, in READINGS IN CYBER ETHICS 430 (Richard A. Spinello & Herman T. Tavani eds., 2001).
[187] *See*, e.g., Aleecia McDonald & Lorrie Cranor, Beliefs and behaviors: Internet users' understanding of behavioral advertising, in 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference), October 2010, http://www.aleecia.com/authors-drafts/tprc-behav-AV.pdf.

While the privacy-as-choice model is perceived as empowering individuals, it in fact often leaves them helpless and confused.[188] Moreover, the binary nature of privacy choices solicited by websites, even with a DNT mechanism (block third party cookies or don't; turn on a header or don't) pale in front of the rich texture of the online behavioral tracking market and fail to capture intricate differences between, for example, "third-party analytics" and "third-party behavioral data collection for first party uses".

Consider the analogy of a patient being asked to consent to a medical procedure. Clearly, if the doctor would throw a medical text book at the patient (which is effectively what websites are doing with privacy policies), she would not be better informed. We expect the doctor to highlight for the patient in plain English and in no more than a few sentences the main risks and perceived benefits of the operation, and allow her to make a decision. To be sure, the patient may choose to pursue additional information by asking follow-up questions, looking for material online, or reaching out to similarly placed patients. But we would not want the doctor to impose such additional information as the default, nor would we impose on patients an obligation to educate themselves in recent medical developments. After having been duly notified and warned, the patient, typically, would at most feel comfortable making a binary "go/no go" decision. And even then, the degree of her volition would be quite limited, given that the vast majority of patients choose what their doctor recommends.

The best interests of patients are protected not so much by lengthy disclosures and comprehensive menus of choices, but rather by medical standards established by regulators and professional associations. In the context of online privacy, this implies emphasis should be placed less on notice and choice and more on implementing policy decisions with respect to the utility of given business practices and on organizational compliance with fair information principles (FIPs). In other words, the focal point for privacy should shift from users to (a) policymakers or self-regulatory leaders to determine the contours of accepted practices; and (b) businesses to handle information fairly and responsibly. This means, businesses must not abuse their information privileges; avoid behavioral tracking of children and the processing of sensitive data; maintain strict limits on data retention; anonymize or pseudonomize databases to the extent possible; never use data to discriminate or inflict harm on users; provide users with transparency and access rights; and implement industry standard methods of data security.

This highlights one of the main differences between United States privacy law and European data protection. United States privacy law is essentially tort law,[189] focused on individuals and

[188] Julie Cohen explains that "[e]ven assuming perfect information about all contemplated reuses of data, however, consumer freedom is relative. Individual consumers are free to accept or reject the terms offered, but it is the vendor who is free to decide what terms to offer in the first place. Thus, consumers may discover that the surrender of personal information is nonnegotiable or prohibitively priced." Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1397 (2000).

[189] William Prosser, Privacy, 48 Cal. L. Rev. 383 (1960); *also see* Restatement (Second) of Torts § 652D (1976); William L. Prosser et al., Prosser and Keeton on The Law of Torts (1984 & Supp. 1988).

providing an *ex post* remedy for harms suffered by them.[190] European data protection law is a regulatory framework, imposing obligations on businesses *ex ante* in order to minimize risk of harm.[191] We agree in this respect with Jacob Kohnstamm, Dutch privacy regulator and head of the Article 29 Working Party, who said: "The fundamental right to data protection cannot be sufficiently guaranteed if the focus lies too much on the actions taken by the individual and on him exercising his individual rights. It is therefore necessary that, in addition to empowering the data subjects and making clearer what their rights are, a strengthening of the duty of controllers by increasing their responsibility to ensure real compliance should take place."[192]

In his classic 1987 article about the foundations of data protection law, Spiros Simitis, who is one of the founding fathers of European privacy regulation and the first data protection regulator, warned against "the chimerical nature of the assumption that effective protection of privacy can be accomplished by simply entrusting the processing decision to the persons concerned (…) The process of consent is no more than a 'mystification' that ignores the long-standing experience that the value of a regulatory doctrine such as 'informed consent' depends entirely on the social and economic context of the individual activity."[193] Policymakers and businesses, not individual users, should shoulder the burden of setting privacy safeguards.

Consent is an elusive concept, somewhat of a wild card in privacy law:[194] On the one hand, it is seldom truly voluntary, since informational privacy is typically implicated in situations of power imbalance – consumer vs. big business; employee vs. employer; and of course citizen vs. the state. On the other hand, consent cannot be entirely done away with, since conceptions of privacy typically incorporate control as a key component, or indeed describe privacy as a form of control over information. This view is usually identified with Alan Westin, who in 1967 defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[195] Clearly, under this approach, consent – the manifestation of individual control - is inextricably tied to

---

[190] Cf. Ryan Calo, The Boundaries of Privacy Harm, 86 Ind. L.J. 1131 (2011).

[191] Ian Walden observes that this "does illustrate a distinction between data protection and privacy law. Under the former, *ex ante* controls are placed on the processing of personal data, whether the information is private or not, while privacy as a tort of misuse is only engaged *ex post*, once an abuse has arisen or is anticipated." Ian Walden, Privacy and Data Protection, *in* Computer Law: The Law and Regulation of Information Technology (Chris Reed & John Angel, Eds., Oxford University Press, 6th Ed. 2007), at p. 463.

[192] Jacob Kohnstamm, New European Rules on Data Protection?, Joint High Level Meeting on Data Protection Day, Jan. 28, 2010, http://ec.europa.eu/justice/news/events/conference_dp_2011/presentations_speeches/panel_1_4_jacob_kohnstamm_speech.pdf.

[193] Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707, 734 (1987).

[194] Omer Tene, You've Been Tagged, Stanford Center for Internet and Society Blog, Mar. 21, 2011, http://cyberlaw.stanford.edu/node/6642.

[195] Alan Westin, Privacy and Freedom (1967), at p. 7. *Also see* Charles Fried, Privacy, 77 Yale L.J. 475, 482 (1968):"Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves"; Arthur Miller, Assault on Privacy (1971), at p. 25: Privacy is the individual's ability to control the circulation of information relating to himself.

privacy.[196] A privacy framework without consent appears overly rigid and paternalistic. In the presence of real, voluntary and informed consent, who is to say that online behavioral tracking, or any other potentially intrusive activity, is illegitimate? After all, online behavioral tracking is not a *mala in se* like organ selling.

One way to rein in the impact of consent is by introducing the concept of "implicit" rather than "explicit" choice, thus recognizing that many default practices are socially acceptable. In its Preliminary Report, the FTC itself reduced the role of consent stating that "[c]ompanies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment."[197] The FTC suggested additional such "commonly accepted practices," including "internal operations" ("websites collect information about visits and clickthrough rates to improve site navigation"); first-party marketing ("online retailers recommend products and services based upon consumers' prior purchases on the website"); fraud prevention; and legal compliance.[198]

A legal assumption of individuals' consent to "commonly accepted practices" is not an FTC innovation. It is already present in European data protection laws, including the Data Protection Directive. One of the fundamental principles of the Data Protection Directive is that personal data may only be collected, used or transferred, if one of a list of enumerated bases is present. The first such legal basis, set forth in Article 7(a) of the Data Protection Directive is consent. Yet Article 7 lists five additional legal bases for processing personal data, at least two of which signify implicit consent.[199] Two additional bases for processing data, compliance with a legal obligation[200] and the legitimate interests of data controllers,[201] do not rely on even a modicum of consent.

The objective, "reasonable person" nature of the "commonly accepted practices" inquiry harkens back to the most celebrated of all legal privacy formula – the "reasonable expectation of privacy" test set forth by the United States Supreme Court in 1967 in *Katz v. United States*.[202]

---

[196] *See* recently Michael Birnhack, A Quest for a Theory of Privacy: Context and Control, 51(4) Jurimetrics __ (forthcoming, 2011).

[197] FTC Preliminary Report, at p. 53.

[198] Ibid, at pp. 53-54. The FTC solicited public comment with respect to the scope of "commonly accepted practices", namely: "is the list of proposed 'commonly accepted practices' described above too broad or too narrow? Additionally, are there practices that should be considered 'commonly accepted' in some business contexts but not in others? Staff also *see*ks comment on the scope of first-party marketing that should be considered a 'commonly accepted practice.' Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing? In addition, should first-party marketing be limited to the context in which the data is collected from the consumer?" Ibid, at p. 56.

[199] Articles 7(b) and 7(d).

[200] Article 7(c) of the Data Protection Directive. *Also see* Section 7 of the Canadian Personal Information Protection and Electronic Documents Act(S.C. 2000, c. 5) (PIPEDA), authorizing collection, use and disclosure of personal information without consent.

[201] Article 7(f) of the Data Protection Directive.

[202] Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

In that landmark decision, Justice Harlan established a two-part test to measure whether a person has a "reasonable expectation of privacy," which is entitled to protection under the United States Constitution.[203] In his famous concurring opinion, Justice Harlan held that the appropriate inquiry is composed of a *subjective prong*, checking whether "a person [has] exhibited an actual (subjective) expectation of privacy" and an *objective prong*, verifying whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[204] It is precisely the objective prong of the *Katz* test, verifying whether "the expectation [is] one that society is prepared to recognize as 'reasonable," which underlies the FTC's willingness to forgo notice and choice for "commonly accepted practices".

The *Katz* test raises problems, however, which similarly impact the FTC's "commonly accepted practices" standard. First, the "commonly accepted practices" test tends to be conservative and may stifle innovation. People typically expect what they know; they do not expect dramatic improvements. In the past, patients did not expect antibiotics; today they may not expect a cure for cancer; or in the online sphere, they did not expect Facebook's News Feed when it was initially launched in 2006.[205] If we interpret "reasonable expectations of privacy" or "commonly accepted practices" as a subjective test, we may obstruct the introduction of value enhancing innovations, such as antibiotics or News Feed. This is not to say that every new buzz is a Facebook News Feed (excuse the pun);[206] but rather that the justification for information practices should sometimes be objective, or normative and determined by policymakers, as opposed to subjective and based on individual choice. A similar point is made by Helen Nissenbaum, arguing that "by putting forward existing informational norms as benchmarks for privacy protection, we appear to endorse entrenched flows that might be deleterious even in the face of technological means to make things better. Put another way, contextual integrity is conservative in possibly detrimental ways (…) It would be problematic if the theory of contextual integrity would judge new forms of information gathering to be a privacy violation in such instances."[207]

A second problem with the subjective aspect of the *Katz* test is that it is logically cyclical and may result in a race to the bottom. Consider an immigrant newly arrived from China to the United States. Such an immigrant may have grown to expect omniscient surveillance by the state; having no subjective expectation of privacy, such an immigrant will be unable to develop a

[203] U.S. Const. amend. IV.
[204] Katz, *supra* note 202, id.
[205] Tracy Samantha Schmidt, Inside the Backlash against Facebook, Time Magazine, Sept. 6, 2006, http://www.time.com/time/nation/article/0,8599,1532225,00.html.
[206] Molly Wood, Google Buzz: Privacy nightmare, Feb. 10, 2010, http://news.cnet.com/8301-31322_3-10451428-256.html#ixzz1Kur3Mn4f.
[207] Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119, 143 (2004). Nissenbaum solves this quandary by proposing that "the requirement of contextual integrity sets up a presumption in favor of the status quo; common practices are understood to reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy (…) A presumption in favor of status quo does not, however, rule out the possibility of a successful challenge where adequate reasons exist." Ibid, at p. 146.

right to privacy under the United States Constitution pursuant to *Katz*. In this way, the *Katz* test becomes a self-fulfilling paranoid prophecy, a slippery slope to a state of no-privacy, since by expecting surveillance one legitimizes the same.[208]

Consequently, policymakers should veer away from futile examination of users' choices and actively cordon-off the limits of consent. Some activities are value creating, socially desirable, and minimally intrusive; they should be permitted to exist as default options. Other activities are privacy intrusive, socially menacing, and may inflict real harm on users; they should be prohibited absent users' informed, explicit, opt-in consent. Where should the line be drawn between "commonly accepted" online practices, and activities which we judge to be harmful and privacy intrusive? The value created by online advertising, which fuels the majority of free content and services available online, as well as the relatively modest harms imposed on users by tailored content, commercial or not; should be assessed against the potentially (real or perceived) detrimental effect online behavioral tracking may have on users' privacy. The necessity of various degrees of data collection and tracking for the measurement necessary for analytics, fraud and ad management should be judged as socially acceptable or as practices to be minimized.

The CDT in effect delineated this threshold in its proposal by defining the meaning of "tracking" under DNT. It demarcates the following practices as "not tracking" (therefore not subject to DNT-type opt-out consent): third-party ad and content delivery; third-party analytics; third-party contextual advertising; first-party data collection and first-party use; federated identity transaction data; specifically excepted third-party ad reporting; and data collection required by law and for legitimate fraud prevention purposes. It refers to the following practices as "tracking" (necessitating a DNT opt-out): third-party online behavioral advertising; third-party behavioral data collection for first party uses; third-party behavioral data collection for other uses; behavioral data collected by first parties and transferred to third parties in identifiable form; and demographic information appended to a user's device.[209] Although framed by a view of the risks created by collection and potential aggregation and use of information, the CDT outcome in effect assigns higher social value to services like analytics and measurement and less to online behavioral advertising. In contrast, proposals by Jonathan Mayer and by Chris Soghoian argue for more limited information collection when a DNT header has been triggered and imply lower social value for behavioral ads in their arguments. Conversely, some in industry

[208] Consider Florida v. Riley, 488 U.S. 445 (1989). The Supreme Court held that police officials do not need a warrant to observe an individual's property via a surveillance helicopter in order to detect marijuana plants in his yard. The Supreme Court reasoned that people do not have a reasonable expectation of privacy from air surveillance because flights have become a common part of our lives.

[209] Center for Democracy & Technology, What Does "Do Not Track" Mean? A Scoping Proposal by the Center for Democracy & Technology, Version 2.0, April 27, 2011, http://www.cdt.org/files/pdfs/20110447_DNT_v2.pdf.

proposed the DNT header trigger an opt-out cookie and indicate an opt-out of targeted behavioral ads, linking DNT to the industry self-regulatory program.[210]

6.2. Enhancing Notice

Transparency is an essential feature of a democratic society, promoting the values of a liberal, political, and social order, as well as being an important FIP. In the context of online behavioral tracking, it has the important effect of counteracting the "creepiness" factor users sometimes feel about industry practices.[211] In addition, the requirement to describe data processing practices in privacy notices led companies to self-examine and professionalize, thus reinforcing adherence to FIPs.

The distinction between transparency as a means for achieving consent and transparency as an independent policy goal is already evident in the introduction to one of the fundamental data protection documents, the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[212] The OECD identifies "Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended" as part of "a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties." Transparency serves not only privacy but also personal autonomy, integrity and dignity.

Ryan Calo noted[213] that there has recently been significant "notice skepticism" based on the fact that privacy notices tend to be long legal documents intended to disclaim corporate liability rather than protecting individual privacy.[214] However, Calo notes that "[n]otice skepticism relies, quite heavily, on certain facts—the human tendency not to read notices; the differences among us in understanding language; and our inherent cognitive limitations such as information overload and wear out—to make the case that notice cannot work. This critique begins to

[210] *See*, e.g., Shane Wiley, Senior Director of Privacy & Data Governance, Yahoo!, W3C Proposal – DAA DNT Hybrid, Do Not Track Headers and CLEAR Ad Notice, Mar. 30, 2011, http://www.w3.org/2011/track-privacy/papers/Yahoo.pdf.

[211] *See*, e.g., Miguel Helft & Tanzina Vega, Retargeting Ads Follow Surfers to Other Sites, NY Times, Aug. 29, 2010, http://www.nytimes.com/2010/08/30/technology/30adstalk.html.

[212] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sep. 23, 1980, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[213] Ryan Calo, Against Notice Skepticism, 87 Notre Dame L. Rev. ___ (forthcoming 2012).

[214] Calo recalls that the Roman emperor Caligula acknowledged the need to create and publish the law, "but it was written in a very small hand, and posted up in a corner so that no one could make a copy of it." Ibid, citing Screws et al. v. United States, 325 U.S. 91, 96 (1945), which itself quotes Suetonius, Lives of the Twelve Caesars 278 (1907). Larry Lessig posits that "the technique of the American government so far—namely, to require text-based privacy policy statements—is a perfect example of how not to act. Cluttering the web with incomprehensible words will not empower consumers to make useful choices as they surf the Web. If anything, it drives consumers away from even attempting to understand what rights they give away as they move from site to site." Lawrence Lessig, Code: Version 2.0 (Basic Books 2006), at p. 228.

unravel if we acknowledge the possibility that experience can change mental models (…) instantaneously, unavoidably, and yet to the same extent as language." He advocates use of "non-linguistic notice," or in his words "[y]ou can write a lengthy privacy policy that few will read, or you can design the website in a way that places the user on guard at the moment of collection or demonstrates to the consumer how their data is actually being used in practice."[215] He calls this "visceral" notice, similar to reintroducing engine noise into otherwise silent electric cars to alert pedestrians, or camera shutter sounds into mobile phone cameras to notify individuals they are being photographed. Similarly, designers can be hired to design websites in ways that make it clear from users' experience what is happening with their data.[216]

Lorrie Cranor, Alessandro Acquisti and a group of researchers at Carnegie Mellon University are working on what they call "privacy nudges," software that essentially sits over users' shoulders and provides them with real-time reminders, such as short on-screen messages, that information they are about to share has privacy implications.[217] Cranor also developed "privacy nutrition labels" to make privacy notices easy to comprehend and compare.[218]

An additional mechanism to improve privacy notices is the behavioral tracking icon. In May 2009, the Future of Privacy Forum[219] launched a research initiative to examine new methods for communicating with users about online advertising and privacy.[220] This study assessed the communication efficacy of behavioral advertising disclosures based on icons and short notices placed near web page advertisements as an alternative to providing transparency and choice via traditional privacy policies. The study employed an internet panel to assess the communication efficacy of behavioral advertising disclosures on the web. It found that transparency and choice increase users' comfort level with online behavioral tracking and that certain icons fared better than others in conveying the message to users. A version of the behavioral tracking icon was adopted by industry in its self-regulatory principles. The IAB Self-Regulatory Principles, for example, require "enhanced notice" under which an entity would "attach a uniform link/icon and wording to each advertisement that it serves. Clicking on this link/icon will provide a disclosure from the entity in the form of an expanded text scroll, a disclosure window, or a separate web page. In this notice, the entity will both disclose its online behavioral advertising

---

[215] Calo, *supra* note 213, at p. 26.

[216] *Also see* Ryan Calo, People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship, 114 Penn St. L. Rev. 809 (2010); Steve Lohr, Redrawing the Route to Online Privacy, NY Times, Feb. 27, 2010, http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html.

[217] *See*, e.g., Alessandro Acquisti, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy Economics, Nov.-Dec. 2009, 82;

[218] Patrick Gage Kelley, Lucian Cesca, Joanna Bres*ee* & Lorrie Cranor, Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach, CMU-CyLab-09-014, Jan. 12, 2010, http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf; Kashmir Hill, Is It Time For Privacy Nutrition Labels?, Forbes.com, Mar. 23, 2011, http://blogs.forbes.com/kashmirhill/2011/03/23/is-it-time-for-privacy-nutrition-labels.

[219] http://www.futureofprivacy.org.

[220] Manoj Hastak & Mary Culnan, Future of Privacy Forum Online Behavioral Advertising "Icon" Study: Summary of Key Results, Jan. 25, 2010, http://futureofprivacy.org/final_report.pdf.

practices and provide a mechanism for exercising choice regarding such practices.[221] The Article 29 Working Party too "acknowledge[d] the work made by some associations such as The Future of Privacy in the context of promoting the use of icons for information purposes."[222]

An additional tool for increasing transparence, privacy dashboards have been designed by online leaders such as Google and Yahoo, to allow users to access categories of data maintained about them and opt-out of marketing based on some or all of these categories.[223] Google states: "With this tool, users can view, add and remove the categories that are used to show them interest-based ads (sports, travel, cooking, etc.) when they visit one of our AdSense partners' websites or YouTube."[224]

Whether it is icons, nutrition labels, dashboards, nudges or visceral notice, transparency can be enhanced in the privacy sphere. More complex notions, such as medical information or tax reporting obligations have been relayed to individuals with varying degrees of success. We all drive cars – massive vehicles of potential destruction – and usually avert disaster, without ever reading the automakers' manuals. This is achieved by deploying product designers to convey to drivers only the most pertinent information required to drive a vehicle (car speed, lights on/off switch, windshield wipers, etc.) The same could be true for privacy notices, which could provide users with real-time information, showing actions as they take place,[225] and giving users an intuitive sense of what goes on behind the scenes of the online market for information.

But the level of effort required to educate or engage with users – whether visceral notice should be delivered as a warning by a scolding face or as an invitation by a smiling character – is driven by an underlying value judgment as to the acceptability of the relevant practice. Visceral notice seeks to elicit an emotional or intuitive reaction based on a perception that a given practice is desirable or not. In contrast, icons and dashboards tend to support data use as a social virtue, seeking to provide information in a non-menacing fashion creating a sense of user trust and control. Indeed, Alessandro Acquisti and colleagues have shown that simply by providing users a

[221] IAB, *supra* note 103, at p. 9. *Also see* Stephanie Clifford, A Little 'i' to Teach About Online Privacy, NY Times, Jan. 26, 2010, http://www.nytimes.com/2010/01/27/business/media/27adco.html.
[222] Opinion 2/2010, *supra* note 85, at p. 16.
[223] Erick Schonfeld, Google Gives You a Privacy Dashboard to Show Just How Much It Knows About You, TechCrunch, Nov. 5, 2009, http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-howmuch-it-knows-about-you; Rob Pegoraro, Yahoo Adds Ad-Preferences Manager, Washington Post, Faster Forward Blog, Dec. 7, 2009, http://voices.washingtonpost.com/fasterforward/2009/12/yahoo_adds_adpreferences_mana.html.
[224] Nicole Wong, Giving consumers control over ads, Google Public Policy Blog, Mar. 11, 2009, http://googlepublicpolicy.blogspot.com/2009/03/giving-consumers-control-over-ads.html.
[225] Consider Ghostery, a popular browser plug-in keeping track of online behavioral tracking and analytics companies. With Ghostery enabled, on every site Ghostery displays a small purple box showing the analytics trackers running on the current page. If something makes a user feel uncomfortable, they can block it. http://www.ghostery.com, stating "Ghostery tracks the trackers and gives you a roll-call of the ad networks, behavioral data providers, web publishers, and other companies interested in your activity."

feeling of control, businesses encourage the sharing of data, regardless of whether or not a user has actually gained control.[226]

Thus the structuring and design of transparency tools, much like choice mechanisms, depend on an implicit underlying value judgment. Advocates averse to online behavioral tracking are unlikely to be satisfied with any implementation of transparency requirements, regardless of how big or bold the fonts are, unless such notices lead to users declining the activity. Once a societal value is set, a wide variety of tools can be used to induce desirable behavior. As Richard Thaler and Cass Sunstein describe in their book *Nudge*, significant changes in human behavior can be provoked by design decisions, such as placing health food at eye level in a cafeteria and demoting fattening food to lower levels.[227] One can only imagine the creative powers that could be unleashed to encourage safe online behavior, if only a national consensus existed about the underlying social values. Absent such consensus, labels and privacy notices, visceral or not, will continue to fail in the eyes of those who dispute the merit of the direction users are "nudged".

6.3. Shifting the burden to business

A better focus for policymakers to take may be shifting the burden of online privacy from users to business, by dimming the highlight on user choice while focusing on businesses' obligations under the FIPs. This signifies a paradigm shift from privacy law to data protection regulation, which, while concerned with privacy, has other goals, such as setting standards for the quality of personal information and ensuring that individuals and businesses are able to process information about others for various legitimate ends.[228]

Lee Bygrave observes that "data protection instruments are expressly concerned with setting standards for the quality of personal information. While adequate information quality can serve to secure the privacy of individuals, it breaks down into a multiplicity of interests (including concern for, *inter alia*, the validity, integrity, availability, relevance and completeness of data) that have little direct connection to privacy-related values."[229] Similarly, Paul Schwartz writes: "The law's chief reaction to these new developments has not been through tort law, but Fair Information Practices (FIPs). This legal response, which began in the United States and Western

[226] Laura Brandimarte, Alessandro Acquisti & George Loewenstein, Misplaced Confidences: Privacy and the Control Paradox, Ninth Annual Workshop on the Economics of Information Security (WEIS) (2010), http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf.
[227] Richard Thaler & Cass Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale University Press, 2008).
[228] Consider the twin (sometime conflicting) goals of the Data Protection Directive as set forth in Article 1: "Object of the Directive – (1) In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. (2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."
[229] Lee Bygrave, Data Protection Law: Approaching its Rationale, Logic and Limits (Kluwer 2002), at p. 163.

Europe in the 1970s, defines obligations for bureaucratic organizations that process personal information (…) Depending on the form that FIPs take, the law can include some combination of enforcement and oversight through a private right of action and governmental enforcement."[230]

Shifting the burden from users to business will have the effect of making online privacy a matter of corporate governance. This trend has already been documented by Deirdre Mulligan and Ken Bamberger, who described the rise of the privacy professional in the United States as a response to FTC enforcement and the increasing influence of privacy advocates, market and media pressures for privacy protection.[231] Mulligan and Bamberger show that by integrating privacy into corporate governance schemes and appointing senior level Chief Privacy Officers as strategic information policy leaders, United States businesses have seen privacy grow from the ground up, whereas European businesses often settle for privacy "on the books". Their research is corroborated by the astounding growth of the International Association for Privacy Professionals (IAPP), the trade association for privacy professionals from a few hundred members at the beginning of the century to more than 8,000 members, a growing number of them from outside the United States, in 2011.[232]

Shifting the burden from users to business will also have a positive effect on the work ethos of privacy professionals. It will make privacy professionals focus more on integrating privacy into products and business processes and less on disclaiming liability for privacy in legal notices. The sad reality is that today, those who care most about privacy are typically engaged in developing an expertise of reducing privacy to unintelligible legal blabber.

In addition to providing clear notice and opt-out tools where necessary, responsible businesses engaged in online behavioral tracking will comply with the following rules:

Sensitive data. Sensitive categories of data should not be used for advertising purposes. Under the Data Protection Directive, the processing of sensitive data ("special categories of data"), including "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," requires explicit individual consent. To preempt the need for elaborate consent requirements, we suggest online behavioral tracking platforms automatically exclude sensitive data categories. We leave for further analysis the definition of what sensitive data means; suffice it to say that medical data and data concerning sexual habits or orientation is sensitive. The use of sensitive data for advertising purposes inherently implies a change of context, unexpected by users except in atypical circumstances. It is precisely this change of context which Helen Nissenbaum

[230] Paul M. Schwartz, Preemption and Privacy, 118 YALE L.J. 902, 907-08 (2009).
[231] Kenneth Bamberger and Deirdre Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247 (2011); *also see* Kenneth Bamberger & Deirdre Mulligan, Catalyzing Privacy: New Governance, Information Practices, and the Business Organization, 33 L. &Pol'y (forthcoming 2011).
[232] Jay Cline, A Call for Agility: The Next-Generation Privacy Professional, International Association of Privacy Professionals, 2010, https://www.privacyassociation.org/images/uploads/IAPP%20Future%20of%20Privacy_Final%20Client.pdf.

forcefully characterized as a privacy infringement.[233] Although industry standards today do limit certain categories of sensitive data, outside the EU these categories are often based on concerns about revenue opportunities or negative publicity, rather than any research into consumer sensitivities or balancing of potential benefits versus privacy risks.

Nissenbaum explains that a privacy violation has occurred when either contextual "norms of appropriateness" or "norms of flow" have been breached. "Norms of appropriateness" dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable or expected to be revealed. For example, it is appropriate to share medical information with a doctor (or friend), but not with an employer or banker. Conversely, it is appropriate to share financial information with an employer or banker, but not with a doctor. Nissenbaum points out that what matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual "norms of information flow". For example, although norms of appropriateness between friends are quite relaxed, allowing for the sharing of almost any information, norms of flow are restrictive, limiting friends from passing on information to others.

Both norms of appropriateness and norms of flow mandate caution before using sensitive data for advertising purposes. Clearly, most users would find offensive being labeled as "Viagra man" or "seeking abortion" and targeted with ads based on such categorization. Exceptions exist, but they cater to very specific audiences and are based on strong opt-in consent. Consider, for example, patients' social networking website PatientsLikeMe.com,[234] which explicitly, conspicuously, and unmistakably holds out to its users a philosophy of openness and use of medical data not only for commercial purposes but also for medical research.[235]

---

[233] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).

[234] http://www.patientslikeme.com.

[235] PatientsLikeMe states in its website under the title "Openness": "**Our Philosophy: Openness is a good thing.** Most healthcare websites have a Privacy Policy. Naturally, we do too. But at PatientsLikeMe, we're more excited about our Openness Philosophy. It may sound counterintuitive, but it's what drives our groundbreaking concept. You *see*, we believe sharing your healthcare experiences and outcomes is good. Why? Because when patients share real-world data, collaboration on a global scale becomes possible. New treatments become possible. Most importantly, change becomes possible (…) Currently, most healthcare data is inaccessible due to privacy regulations or proprietary tactics. As a result, research is slowed, and the development of breakthrough treatments takes decades. Patients also can't get the information they need to make important treatment decisions. But it doesn't have to be that way. When you and thousands like you share your data, you open up the healthcare system (…) PatientsLikeMe enables you to effect a sea change in the healthcare system. We believe that the Internet can democratize patient data and accelerate research like never before. Furthermore, we believe data belongs to you the patient to share with other patients, caregivers, physicians, researchers, pharmaceutical and medical device companies, and anyone else that can help make patients' lives better". http://www.patientslikeme.com/about/openness.

Children's data. In our view, children should not be subject to online behavioral tracking. Children are a vulnerable target audience since they lack the capacity to evaluate ads and comprehend the data exchange underlying online transactions, particularly the potentially long-term effects of the data they divulge.[236] This is also the position of the European Article 29 Working Party, which states that "taking into account the vulnerability of children, the Article 29 Working Party is of the view that ad network providers should not offer interest categories intended to serve behavioral advertising or influence children."[237]

Under the Children's Online Privacy Protection Act (COPPA),[238] businesses should not collect personal information from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13, or engage in online behavioral advertising directed to children they have actual knowledge are under the age of 13, except as compliant with the COPPA. This may not be enough. Privacy advocates note: "Children are increasingly subjected to a wide array of behavioral targeting practices through social networks, games, mobile services, and other digital platforms that use techniques that evade current legal restrictions. Scholars in neuroscience and psychology have identified a number of biological and psychosocial attributes that make adolescents particularly vulnerable to behavioral targeting."[239] Many responsible behavioral advertising companies already refrain from creating profiles from visits to sites directed at children under 13, even without actual knowledge of children's use of such sites, which triggers the provisions of COPPA. Industry standards, meanwhile, track COPPA and only limit behavioral ads when there is actual knowledge of the individual's age. These restrictions should be extended to fully limit even anonymous behavioral ads on such sites or creating profiles from data gleaned from users of children's sites.

Anonymization/Psuedonymization. To the maximum possible extent, businesses engaged in online behavioral tracking should avoid processing personal information. This can be achieved, for example, by truncating IP addresses and hashing user IDs, to provide a non-personal information state management scheme. Nevertheless, even with anonymized data, all additional privacy by design measures must be maintained, given the robust de-anonymization attacks highlighted in recent computer science and legal literature.[240] For example, law

---

[236] Alice Marwick, Diego Murgia Diaz & John Palfrey, Youth, Privacy, and Reputation (Literature Review), Berkman Center Research Publication No. 2010-5, Harvard Public Law Working Paper No. 10-29 (2010), http://ssrn.com/abstract=1588163.

[237] Opinion 2/2010, *supra* note 85, at p. 17.

[238] 15 U.S.C. §§ 6501–6506 (2006).

[239] Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group & The World Privacy Forum, Online Behavioral Tracking and Targeting, Legislative Primer September 2009, http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf. *Also see* Deborah Moscardelli & Catherine Liston-Heyes, Teens Surfing The Net: How Do They Learn to Protect their Privacy? 2(9) Journal of Business and Economics Research 43 (2004).

[240] Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy 111; Michael Barbaro & Tom Zeller, A Face is Exposed for AOL

professor Paul Ohm observed that "clever adversaries can often re-identify or de-anonymize the people hidden in an anonymized database… Re-identification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization."[241]

No discriminatory non-marketing related uses. Far more troubling than the use of online behavioral tracking for ad targeting purposes is the use of online tracking for decisions in the fields of employment, insurance, banking and litigation. The use of a user's browsing information in order to price her insurance premiums (*e.g.*, based on her reading an article about breast cancer on Wikipedia or WebMD) or mortgage rates (*e.g.*, based on her visiting bankruptcy advice websites) constitutes illegitimate context change and may inflict tangible harm on users. Helen Nissenbaum would characterize the transfer of information about online browsing to information brokers a breach of "norms of flow."[242] "According to the theory of contextual integrity, it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."[243] It is important to ask whether the information transfer harms users; interferes with their self-determination; or amplifies undesirable inequalities in status, power, and wealth. The prevention of unexpected uses of data is also mandated by existing data protection legislation, such as Article 6(1)(b) of the Data Protection Directive, which requires that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

Retention. Much has been written recently about the so called "right to oblivion" or "the right to be forgotten". Indeed, in outlining the "four pillars" for the revised European data protection framework, Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner recently stated that "[t]he first [pillar] is the 'right to be forgotten': a comprehensive set of existing and new rules to better cope with privacy risks online. When modernizing the legislation, I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need

---

Searcher No. 4417749, NY Times, August 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html.

[241] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010).

[242] Emily Steel, A Web Pioneer Profiles Users by Name, Wall Street Journal, Oct. 25, 2010, reporting: "RapLeaf knows even more about (…) millions of other Americans: their real names and email addresses. This makes RapLeaf a rare breed. Rival tracking companies also gather minute detail on individual Americans: They know a tremendous amount about what you do. But most trackers either can't or won't keep the ultimate piece of personal information—your name—in their databases. The industry often cites this layer of anonymity as a reason online tracking shouldn't be considered intrusive. RapLeaf says it never discloses people's names to clients for online advertising. But possessing real names means RapLeaf can build extraordinarily intimate databases on people by tapping voter-registration files, shopping histories, social-networking activities and real estate records, among other things."

[243] Nissenbaum, *supra* note 207, at p. 154-55.

to keep the data rather than individuals having to prove that collecting their data is not necessary."[244] The principle of retention limitation, as already embodied in Article 6(1)(e) of the Data Protection Directive, requires personal data to be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." In its Green Paper, the Department of Commerce advocated adoption of a data minimization principle under which companies "only retain personal information for as long as is necessary to fulfill the specified purpose(s)."[245]

Accordingly, data provided to companies engaged in online behavioral tracking should be subject to a regular deletion policy. The length of the retention period, for example one week or one year, makes not only a quantitative but also a qualitative difference with respect to the impact of the data profile on user privacy. If a particular user does not interact with a tracking platform for a certain period of time, to be determined according to functional and technical specifications, their data should be deleted. Interacting with the platform once again will result in a new call for data.

Access and rectification. Transparency entails providing users not only with information about data collection, use and transfer practices, but also with access to any files held by business about them and an opportunity to correct any data which are inaccurate or incomplete. For example, Article 12 of the Data Protection Directive grants individuals the right to access certain basic information from businesses about the storage, use and transfer of their personal data, and rectify any information which is inaccurate. Access and rectification rights are recognized as FIPs in documents ranging from the 1980 OECD Guidelines[246] to the 2008 United States Department of Homeland Security Privacy Policy Guidance Memorandum.[247] To the extent websites, advertisers or ad intermediaries maintain user profiles which can be identified to specific individuals, those individuals should be afforded with access and rectification rights.

Data security. Article 17 of the Data Protection Directive imposes the obligation on companies to apply "technical and organizational measures" to protect personal data against unauthorized or unlawful access or use, or accidental loss or destruction. In the United States, security breach notification laws have been enacted in most states and are now considered at the national

[244] Viviane Reding Vice-President of the European Commission, EU Justice Commissioner, Your data, your rights: Safeguarding your privacy in a connected world Privacy Platform, The Review of the EU Data Protection Framework, Brussels, Mar. 16, 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183.

[245] The Department of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, December 16, 2010, www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[246] Article 13 to the OECD Guidelines, titled "Individual Participation Principle".

[247] Department of Homeland Security Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, Dec. 29, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf, referring to the "Individual Participation" principle.

level.[248] Businesses engaged in online behavioral tracking must implement appropriate data security measures to comply with industry standards and best practices necessary to protect data of the type and amount used by their platforms.

Accountability. With the proliferation of cross border data transfers and the advent of cloud computing, policymakers on both sides of the Atlantic have called for reiteration of the accountability principle.[249] Under the accountability principle, initially introduced in the 1980 OECD Guidelines, an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Given that the online behavioral tracking platforms entail multi-party cross border data transfers, businesses must introduce contractual and organizational accountability measures.

7. Conclusion

The past decade has seen a proliferation of online data collection, processing, analysis and storage capacities leading businesses to employ increasingly sophisticated technologies to track and profile individual users. Tracking may be performed for various purposes, including protecting and securing services from fraud and abuse, determining the relevancy of served content, providing accurate measurement of the impact of commercial and non-commercial content, and targeting behaviorally tailored ads. The use of online behavioral tracking for advertising purposes has drawn criticism from journalists, privacy advocates and regulators. In particular, critics argued that users are uninformed of industry information practices and deprived of the opportunity to exert meaningful control over their data. This has led to regulatory and self-regulatory proposals to increase transparency and enhance user choice, most notably the FTC DNT proposal in the United States and the amendment to the e-Privacy Directive requiring opt-in consent for the use of cookies in the EU.

We argue that the debate raging on both sides of the Atlantic needs to be informed by a discussion of the fundamental tradeoff between privacy and economic efficiency. By focusing on the mechanics of notice and choice, participants in the debate have effectively saddled users with a difficult policy decision they are ill equipped to make. Whether a given practice requires opt-in, opt-out or no consent; and if so where and how choices should be presented;

[248] The Department of Commerce Green Paper advocates "the consideration of a Federal commercial data security breach notification law that sets national standards, addresses how to reconcile inconsistent State laws, and authorizes enforcement by State authorities." (p. 7).

[249] Article 29 Data Protection Working Party, Opinion /2010 on the principle of accountability, WP 173, July 13, 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf; Department of Commerce Green Paper, pp. 26, 30-31, 40-41, 56. The accountability principle appears in Canadian federal privacy legislation; *see* the Personal Information Protection and Electronic Documents Act (PIPEDA), (S.C. 2000, c. 5), Schedule 1, Principle 4.1, titled "Accountability".

camouflage deep value judgments which have yet to be made. This is not to say that a value judgment needs to be as stark as a binary choice between privacy and efficiency. On the contrary, a more nuanced equilibrium is needed taking into account the benefits of not only privacy rights but also access to information and services, freedom of speech and economic efficiency. Such a balance would then be used to draw the line between practices that are acceptable without prior consent and those that require more purposeful engagement by users.

Instead of shifting the burden to users, policymakers and self-regulatory leaders should coalesce around a common approach to the information-for-value business model currently prevailing online. If this model is seen as positive from a societal point of view, then online behavioral tracking should be accepted as a default, with opt-out options available via advanced browser settings and implemented by industry self-regulatory programs. Conversely, if the information-for-value model is viewed as a perverse monetization of users' fundamental rights, then aspects of it should be curbed by prominent opt-out or opt-in requirements. We suggest placing a primary emphasis on reaching consensus on the policy outcome in order to effectively guide the development of consumer choice mechanisms, and then assigning fair and responsible data use obligations to businesses.