RECENT DEVELOPMENT

TO TRACK OR NOT TO TRACK: RECENT LEGISLATIVE PROPOSALS TO PROTECT CONSUMER PRIVACY

I. INTRODUCTION

Ten years ago, there was no Facebook. Google had not emerged as the dominant email client, search engine and jack-of-all trades that it is today. Consumers in search of bargains still clipped coupons rather than waiting for the perfect Groupon deal. Despite this constant increase in online activity, however, Congress has consistently failed to pass legislation that would protect consumer privacy online. Bills were introduced as early as 2000 that would have implemented a comprehensive set of online privacy protections, but they did not become law.[1]

This session, consumer protection online is on the legislative calendar yet again.[2] The full universe of legislation includes bills addressing consumer privacy online, data breach notification/security, children's privacy, amendments to the Electronic Communications Privacy Act, geolocation privacy, and financial privacy.[3] This Note evaluates[4] two of the general privacy bills, the Commercial Privacy Bill of Rights and the Do Not Track Online Act, and concludes that the Commercial Privacy Bill of Rights will ultimately provide the best protection for consumers, while preserving the vibrancy and generativity of the Internet.

II. THE CURRENT PRIVACY CLIMATE: UNREGULATED BEHAVIORAL TRACKING

Recent legislative attention to consumer privacy online can be explained, in part, by the increasing use of behavioral tracking online over the past decade. Personal information has become "commodified"; that is, it is "bought, sold, or otherwise exchanged for corporate gains."[5] As new tech-

---

[1] *See, e.g.*, Consumer Privacy Protection Act of 2000, S. 2606, 106th Cong. (2000).

[2] *See, e.g.*, Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Do Not Track Online Act of 2011, S. 913, 112th Cong. (2011); Data Accountability and Trust Act, H.R. 1707, 112th Cong. (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011); BEST PRACTICES Act, H.R. 611, 112th Cong. (2011).

[3] *Id.*

[4] I evaluate these bills assuming that the technical aspects of both are unproblematic, although both bills may in fact present technical challenges. For the purposes of this Note, I focus on the policy aspects of the bills.

[5] Shubhankar Dam, *Remedying a Technological Challenge: Individual Privacy and Market Efficiency; Issues and Perspectives on the Law Relating to Data Protection*, 15 ALB. L.J. SCI. & TECH. 337, 340 (2005). Two major technological shifts made this possible: (1) the

nologies allow consumers to access content on demand and bypass unwanted advertisements, capturing the consumer's attention for these fleeting seconds has become increasingly competitive. Targeted advertising is one of the most effective ways to attract the consumer's attention; rather than showing the consumer a generic ad, the marketer can select an ad relevant to the consumer's demographic group or previously expressed interests.[6] Using this method, the consumer is more likely to watch (and even respond to) the ad and the marketer is more likely to make a sale.[7]

The data collection that this kind of advertising relies on takes a number of different forms,[8] some more transparent than others. The most transparent model is the "direct collection" or "first party" model, whereby a company like Netflix or Google makes personal recommendations to a user by taking information that the user has provided and comparing it with other users' information.[9] The next model is the "cookie-based" model,[10] which remembers the consumer's identity across visits to multiple web pages (e.g., when the consumer adds items to a shopping cart).[11] This technology can also collect information about the consumer that a network advertiser can use to supply the most relevant ads.[12] The final two tracking methods—the "spyware-based" and "deep packet inspection" approaches—are much more difficult to detect. Neither provides the user with explicit notice that his or her online activity is being monitored.[13] Spyware is often installed in the course of typical Internet usage without the user knowing that anything

---

advent of computer data banks in the 1960s; and (2) the proliferation of Internet technology in the 1990s. *Id.*

[6] FEDERAL TRADE COMMISSION, PROTECTING CONSUMERS IN THE NEXT TECH-ADE: A REPORT BY THE STAFF OF THE FEDERAL TRADE COMMISSION 10 (2008) [hereinafter NEXT TECH-ADE], *available at* http://ftc.gov/os/2008/03/P064101tech.pdf.

[7] *Id.*

[8] Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 7 (2010).

[9] *Id.* at 15–16.

[10] While many consumers are familiar with and have become critical of this model, it is not always easy to avoid. Although most web browsers allow their users to disable cookies, some websites do not work without them, leading consumers to avoid such blanket protections. *Id.* at 10.

[11] [W]ebsite developers often must use cookies to identify a web browser between requests for web pages because the hypertext transfer protocol, which describes the rules computers follow when they load web pages, is "stateless." This means that a website developer wants to create a process that remembers the consumer's identity across visits to multiple web pages (the procedure of adding items to an online shopping cart is the paradigmatic example of this), the website developer must use cookies (or some other means) to distinguish the consumer from other consumers and remember the context of that consumer's earlier visits.

Id.

[12] *Id.* at 7–9. Many businesses that use "cookie-based" behavioral advertising employ the services of "network advertisers." These companies select and deliver advertisements to websites that are members of their networks. All sites within a given network provide information about a certain user, allowing a network advertiser to create a "rich profile" connected to a given consumer's IP address. *Id.* at 8.

[13] *Id.* at 11.

on his or her computer has changed. Internet service providers (ISPs) often install "deep packet inspection" hardware without consumer knowledge.[14] Even if the consumer realizes that his or her computer has spyware on it, the consumer may be unable to delete it effectively.[15]

Current laws do little to assuage consumer fears of being tracked online, in spite of consistent warnings from commentators that a completely unregulated space may destroy consumer trust in the Internet.[16] Data and privacy protection law at the federal level in the United States operates on a sector-specific basis, with different federal laws governing different industries.[17] For instance, the Children's Online Privacy Protection Act ("COPPA")[18] covers the protection of children online; regulations promulgated under the Health Insurance Portability and Accountability Act ("HIPAA")[19] govern the release of medical information; and the Gramm-Leach-Bliley Act ("GLB")[20] covers the privacy of consumer information retained by financial institutions.[21] A patchwork of state laws currently fills the gaps inherent in the sectoral approach. Generally, these laws require consumer notification in the event of an information breach, but they do not provide protections for the use of consumer data.[22] The primary function of data breach notification is to "provide individuals with an opportunity to mitigate any potential adverse outcomes, thus assisting with the prevention

---

[14] *Id.* at 12.

[15] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 53–54 (2008) (describing how some programs downloaded from the Internet install hidden extras in the form of spyware that can be incredibly difficult to uninstall without expert knowledge).

[16] *See, e.g.*, Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 28–30 (2006) (suggesting that a lack of regulation could result in a "tragedy of the commons" scenario in which consumers would pull back from the Internet); Dam, *supra* note 5, at 346 ("The direction in which privacy law evolves will largely determine the public's confidence in certain systems of communication including the Internet. Without adequate protection trade via the Internet may itself be the eventual casualty.").

[17] Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 65 (referring to the sectoral approach to information privacy adopted by the United States); *accord* Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 812 (2003).

[18] 15 U.S.C. §§ 6501–6506 (2006).

[19] 45 C.F.R. pt. 160, 164 (2010).

[20] 15 U.S.C. §§ 6801–6809 (2006).

[21] The HIPAA Privacy Rule is currently going through notice-and-comment rulemaking. The comment period opened May 31, 2011. The proposed rule would give people the right to receive a report on who has accessed their protected health information. HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31,426, 31,426–31,449 (proposed May 31, 2011) (to be codified at 45 C.F.R. pt. 164).

[22] *See, e.g.*, Burdon, *supra* note 17, at 65 ("Data breach notification laws were developed in the absence of a comprehensive data protection framework as a specific law for a particular problem"; that is, the mitigation of identity theft). For representative examples of state laws, *see* CAL. CIV. CODE § 1798.29 (West 2003); D.C. CODE § 28-3851 (West 2007); and MASS. GEN. LAWS ch. 93H § 1 (2007).

of identity theft-related [sic] crimes."[23] Currently, the entity whose files were compromised shifts the burden of data protection onto the individual consumer. The consumer must "mitigate any potential adverse outcomes," though he or she never had the opportunity to prevent the data breach in the first place. The consumer may never even know the breadth of information that has been compromised, as much data collection takes place surreptitiously.

The Federal Trade Commission (the "FTC") also plays a major role in the public debate over behavioral tracking.[24] Since 1995, it has encouraged and evaluated self-regulatory attempts to protect consumer privacy through principles that it updates and distributes on a regular basis.[25] The FTC's current set of self-regulatory principles lacks a traditional enforcement mechanism.[26] Any attempt to prosecute a private company's actions must instead arise from the FTC's limited jurisdiction in the Federal Trade Commission Act (the "FTC Act").[27] Under the basic consumer protection provision of the FTC Act, the FTC can only take action if a company's acts or practices are "unfair or deceptive."[28] The FTC's jurisdiction over "unfair" acts or practices includes those that unfairly cause injury or a reasonable likelihood of injury.[29] The typical Internet privacy case does not fit neatly within this unfairness jurisdiction.[30] For a practice to be deceptive, a company must have promised one thing and then done another.[31] For example, if a company promised certain protections in its privacy policy and breached that promise,

---

[23] Burdon, *supra* note 17, at 78.

[24] Norian, *supra* note 17, at 819.

[25] *Id.* The most current set of principles dates to 2009 and is reported in FEDERAL TRADE COMMISSION, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: TRACKING, TARGETING, AND TECHNOLOGY (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[26] *See generally id.*

[27] *See infra* note 30; *cf.* NEXT TECH-ADE, *supra* note 6, at 26.

[28] 15 U.S.C. § 45(a)(1) (2006).

[29] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 40 n.111 (2010) [hereinafter FRAMEWORK], *available at* http://ftc.gov/opa/2010/12/privacyreport.shtm.

[30] *See Privacy and Data Security: Protecting Consumers in the Modern World*, *Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 112th Cong. (2011) [hereinafter *Privacy Hearing*], video *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=e2c2a2ca-91d6-48a2-b5ea-b5c4104bdb97&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b6c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=6&YearDisplay=2011 (FTC Commissioner Julie Brill testifying that if a company failed to honor a consumer's "do not track" request using current web browser technology, the FTC would have difficulty prosecuting the company under the FTC's unfairness jurisdiction because "if a company does not make a promise to adhere to a consumer's request then our jurisdictional test is a little bit more difficult to meet. We fall under our unfairness jurisdiction and there are some challenges in meeting that kind of a test.").

[31] *See* Brian Stallworth, *Future Imperfect: Googling for Principles in Online Behavioral Advertising*, 62 FED. COMM. L.J. 465, 480 (2010) ("The FTC watches for deceptive trade practices by holding online businesses to their word, requiring them to keep the promises they made to consumers."). In order to prove a deceptive act or practice, the FTC must demonstrate three elements: "(1) a representation, omission, or practice, that (2) is likely to mislead consumers acting reasonably under the circumstances, and (3) the representation, omission, or

the FTC would have jurisdiction to bring suit against the company.[32] Although the FTC has found limited ways to adapt the current framework to address privacy concerns, its commissioners believe that comprehensive data privacy legislation would better protect consumers.[33]

Despite increased Internet usage and increased opportunities for privacy breaches, some policymakers worry that data protection legislation is little more than "a solution in search of a problem."[34] They suggest that the dour predictions that the Internet will cease to entice consumers without more privacy protections are overblown.[35] Consumer behavior and industry recommendations, however, reveal how essential it is to maintain consumer trust in the Internet. For one, a majority of consumers would prefer to have greater control over what information they share online. A 2008 poll by the Consumer Report National Research Center found that a majority of Americans were concerned about the use of their personal information online; specifically, seventy-two percent were "concerned that their online behaviors were being tracked and profiled by companies."[36] Sixty-five percent of Americans have changed their privacy settings on social networks to limit what they share online.[37] Young people are likely to adjust their Facebook privacy settings to restrict the data they share with others, challenging the idea that we live in an era of shifting privacy norms.[38] Industries that rely on the Internet have also acknowledged that consumer trust is essential to com-

---

practice is material." FTC v. Verity Int'l, Ltd. 443 F.3d 48, 63 (2d Cir. 2006) (quoting *In re* Cliffdale Assocs., 103 F.T.C. 110, 165 (1984)).

[32] *See, e.g., In re* Geocities, Inc., 127 F.T.C. 94 (1999) (consent order) (settling charges that website misrepresented the purposes for which it was collecting information from children and adults); FTC v. Toysmart.com, LLC, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (consent order) (challenging website's attempts to sell children's personal information, notwithstanding a promise in its privacy policy that such information would not be disclosed); *In re* Petco Animal Supplies, Inc., 139 F.T.C. 102 (2005) (alleging that Petco failed to comply with a posted privacy policy).

[33] The FTC's current proposed framework, released last December after a number of roundtables, suggests the following principles to guide consumer privacy protection: (1) Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services; (2) Companies should simplify consumer choice; and (3) Companies should increase the transparency of their data practices. FRAMEWORK, *supra* note 29.

[34] *Privacy Hearing*, *supra* note 30 (statement of Sen. Toomey (R-Pa.)).

[35] *Id.*

[36] Press Release, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMERSUNION (Sept. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

[37] MARY MADDEN & AARON SMITH, PEW RES. CTR., REPUTATION MANAGEMENT AND SOCIAL MEDIA: HOW PEOPLE MONITOR THEIR IDENTITY AND SEARCH FOR OTHERS ONLINE 3, 45 (2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf.

[38] Danah Boyd & Ezster Hargittai, *Facebook Privacy Settings: Who Cares?*, FIRST MONDAY (Aug. 2, 2010), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589 ("Our results challenge widespread assumptions that youth do not care about and are not engaged with navigating privacy. We find that, while not universal, modifications to privacy settings have increased during a year in which Facebook's approach to privacy was hotly contested.").

mercial activities on the Internet and that "erosion of trust will inhibit the adoption of new technologies."[39] Thus, to preserve the Internet's power and utility, privacy legislation is imperative.

III. The Proposed Legislation[40]

The Commercial Privacy Bill of Rights Act of 2011 ("CPBR"), introduced by Senator John Kerry (D-Mass.) and co-sponsored by Senator John McCain (R-Ariz.), represents one approach to protecting consumer privacy. It seeks to "establish a regulatory framework for comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission."[41] The CPBR would require companies that collect consumer data to adhere to certain security practices and would also require consumers to opt-in to the collection of sensitive information.[42] Consumers could also access, correct, and control information that companies have stored.[43] In addition, the bill would limit the data that a company could collect during any given transaction to only data that is necessary for the transaction's completion.[44] For instance, an online shoe store could not require the consumer to provide personal information such as his or her birthday if such information is tangential to the consumer's purchase of snow boots.

Though the CPBR represents a serious bipartisan effort to protect consumer privacy, it came under fire from several consumer groups for failing to include a "do not track" mechanism.[45] A "do not track" mechanism—similar to the "do not call" list established to protect consumers from unwanted marketing phone calls—would allow consumers to entirely opt-out of online tracking. With one click, the consumer could tell any online entity that he or she does not want personal data collected or a profile created that details his or her online habits.

---

[39] Internet Policy Task Force, U.S. Dep't of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework 15 (2010), *available at* http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf (summarizing industry responses to the notice of inquiry, which overwhelmingly support measures that will increase consumer trust in the Internet).

[40] I focus on two particular bills that have attracted some attention this session, but the points raised here are generalizable to other pieces of legislation that include similar provisions, such as the "do not track" provision.

[41] 157 Cong. Rec. S2387 (daily ed. Apr. 12, 2011).

[42] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 202(a)(3)(A) (2011). The bill defines "sensitive personally identifiable information" as "personally identifiable information which, if lost, compromised, or disclosed without authorization either alone or with other information, carries a significant risk of economic or physical harm" or information related to an individual's medical conditions or religious affiliation. *Id.* § 3(6).

[43] *Id.* § 202(a)(4).

[44] *Id.* § 301(1).

[45] Tanzina Vega, *Senators Propose New Privacy Law*, Media Decoder (Apr. 12, 2011, 6:43 PM), http://mediadecoder.blogs.nytimes.com/2011/04/12/senators-propose-new-online-privacy-law/.

The Do Not Track Online Act of 2011 (the "DNTOA"), on the other hand, does include such a mechanism. The DNTOA was introduced by Senator John D. Rockefeller (D-W. Va.) and it "[establishes] the sense of Congress that Congress should enact, and the President should sign, bipartisan legislation to strengthen public safety and to enhance wireless communications."[46] As its title suggests, the legislation would require a mandatory browser-based "do not track" mechanism that would allow consumers to opt-out of online information collection.[47]

IV. What's a Legislature to Do?

The CPBR and the DNTOA share a goal, but they fundamentally differ in certain respects. As mentioned above, the CPBR does not explicitly include a "do not track" mechanism, even though it adopts other mechanisms to safeguard consumer privacy.[48] In addition, the CPBR is a much more comprehensive piece of legislation and one that will fit better with the existing Internet architecture. Finally, the CPBR includes innovative co-regulatory measures that will help ensure that regulations promulgated by the FTC remain relevant and appropriate. For these reasons, the CPBR represents a better approach to consumer privacy.

A. To Track or Not to Track?

The most obvious difference between the two proposed pieces of legislation is the absence of a "do not track" mechanism in the CPBR. The "do not track" mechanism is appealing because it is easily articulable and addresses the problems many consumers have with the current Internet climate. For instance, a poll conducted by *Consumer Reports* found that 81% of respondents believed they should be able to permanently opt-out of Internet tracking.[49] "Do not track" provisions, however, are a blunt tool for a

---

[46] 157 Cong. Rec. S2777 (daily ed. May 9, 2011).

[47] Tanzina Vega, *Do Not Track Privacy Bill Appears in Congress*, Media Decoder (May 6, 2011, 5:01 PM), http://mediadecoder.blogs.nytimes.com/2011/05/06/do-not-track-privacy-bill-appears-in-congress/. Other bills also provide for a "do not track" mechanism, including the Do Not Track Kids Act of 2011, introduced by Representatives Ed Markey (D-Mass.) and Joe Barton (R-Tex.), the co-chairmen of the bipartisan Congressional Privacy Caucus. *Do Not Track Kids Act of 2011*, H.R. 1895, 112th Cong. (2011). An FTC report in December 2010 called for a similar mechanism, leading several major browser distributors, including Google and Mozilla, to introduce features that would allow users of their browsers to opt out of being tracked online. Tanzina Vega, *Google and Mozilla Announce New Privacy Features*, Media Decoder (Jan. 24, 2011, 12:52 PM), http://mediadecoder.blogs.nytimes.com/2011/01/24/google-and-mozilla-announce-new-privacy-features/. As of today, only one company, the Associated Press, appears to respect the browser mechanism. *Privacy Hearing*, *supra* note 30.

[48] Though not explicit in the bill, administrative officials have discussed the possibility of developing a "do not track" mechanism through a co-regulatory process. *See infra* text accompanying notes 73–80.

[49] Consumer Reports Nat'l Res. Ctr., Project No. 2011.55, Final Report: Internet Privacy Poll, (forthcoming) (available upon request from Consumers Union).

nuanced and ever-evolving problem. At the same time, the DNTOA provisions may permit data collection by methods other than tracking. Thus while customers may believe that they are adequately protected by this legislation, companies may continue infringing on their privacy.

On its face, the DNTOA seems like a boon to consumers concerned about their privacy. What could be better than to ban tracking, which makes so many consumers uncomfortable? This kind of proposal, however, fails to take into account the many benefits that consumers receive from tracking done right.[50] Behavioral advertising, for instance, greatly improves the efficiency of advertising, helping small businesses reach their target demographics and giving consumers easy access to relevant, useful advertisements.[51] Though all information may not be collected for proper purposes or used in ways that make a consumer comfortable, giving consumers an easy way to opt-out of tracking may reduce the economic incentive for Internet content providers that rely on advertising for revenue to maintain their sites and other content.[52] Advertisers are currently willing to pay more for targeted advertising, which is made possible by online tracking. If online tracking is diminished by the DNTOA's proposed method, the consumer-content provider relationship will have to change: either consumers will have to see more ads, or consumers will have to pay for formerly free online services.[53] This may leave consumers in a situation similar to that of consumers who, in today's Internet environment, opt to turn off cookies on their browsers.[54] Similarly, the environment created by a "do not track" bill could leave consumers with a choice between ceding control over their personal information and having access to a severely reduced Internet experience—one in which websites fueled by ad revenue are essentially closed off to them.[55]

---

[50] Even FTC Commissioner Julie Brill acknowledged the many benefits that can flow from a more customized Internet experience in testimony before the Senate Commerce, Science, and Transportation Committee. *Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 112th Cong. (2011) (statement of Julie Brill, Comm'r, FTC), *available at* http://commerce.senate.gov/public/index.cfm?p=hearings. While endorsing the idea of a "do not track" mechanism, Commissioner Brill also noted that the consumer "enjoys free and immediate access to information, locates places of interest, obtains discounts on purchases, stays connected with friends, and can entertain herself and her family. Her life is made easier in a myriad of ways because of information flows." *Id.*

[51] Berger, *supra* note 8, at 31–32.

[52] *See id.* at 50.

[53] *Id. See also Privacy Hearing*, *supra* note 30 (statement of Thomas M. Lenard, President and Senior Fellow, Technology Policy Institute), *available at* http://commerce.senate.gov/public/index.cfm?p=hearings ("[T]he information generated by online tracking generates positive externalities that support the services that everyone uses. Consumers who opted for a Do-Not-Track mechanism might be free-riding off those customers who allowed their data to be used.").

[54] *See supra* note 10.

[55] *See* Berger, *supra* note 8, at 50. *Cf.* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1266 (1998) (noting that a significant pitfall to a rule forbidding a company from conditioning a cyberspace transaction on surrendering information

Restricting consumer access to the Internet may fundamentally change the online experience. The Internet has become such a force for good and ill because of its "generativity." That is, the Internet functions as a platform that "invite[s] people to tinker with it."[56] The generativity that has allowed for the Internet's great success may also be its downfall; as Professor Zittrain notes, this characteristic of the Internet also allows people to "tinker" in a malicious way, by writing codes that infect computers and cause them to perform unwanted tasks.[57] Ultimately, he argues, this kind of bad faith use of the Internet could turn many users away. The Internet was initially built on trust,[58] and multiple breaches of that trust could "threaten the very foundations of the generative system."[59] By failing to reinforce this trust—through consumer protection online legislation, for example—we fail to protect a resource that has changed the way our world works over the course of just a few decades.

However, by allowing any consumer to completely opt-out of tracking, "do not track" mechanisms focus only on a very specific method used to glean information about consumers. While such mechanisms would address the often surreptitious data collection that occurs today, they would not address, for example, the situation in which consumer information is collected as consideration for access to a website.[60] Reliance on a currently common data collection method does not guarantee consumer privacy. Rather, it cuts off one head of what may fairly be characterized as a hydra: if you take off one head, one or more will grow in its place.[61]

Government regulation often seems clumsy in the face of the rapid innovation that characterizes today's Internet. A law like DNTOA, which focuses closely on a specific method of collecting consumer information, may

---

privacy is the predictable response of the company: charging penalties to those who do not consent to information collection).

[56] ZITTRAIN, *supra* note 15, at 2.

[57] *Id.* at 36–52.

[58] *Id.* at 31–32.

[59] *Id.* at 43.

[60] For an example of this, see Dam, *supra* note 5, at 345 (Information "is often collected during transactions on the Internet. Such information may be ancillary to the actual transaction or may be the consideration for the transaction itself. Free web pages that provide customized service require [personal information] as 'payment' for accessing the content of the data collector's site.").

[61] For a critique of this method of data collection regulation, see Burdon, *supra* note 17, at 103.

> The law's focus on process has the benefit of providing a manageable and implementable set of fair information principles that can readily translate to a regulatory mechanism but it relegates the protection of privacy to limited circumstances and thus greatly reduces the potential scope for legal redress or remedial action. The inherently reductionist scope of information privacy law has created the situation in which even legislative rights granted through the law are nonetheless limited because they are based on mechanistic processes of personal information exchange.

Id.

fall flat.[62] While the bill is appealing because it offers a straightforward, easily explained solution to the privacy problem, its implementation would open the door to serious consequences for the Internet experience.

B. The Commercial Privacy Bill of Rights: A Balanced Solution

In contrast to the DNTOA, the CPBR represents a nuanced approach to balancing the privacy interests of consumers, while at the same time retaining many of the benefits of online tracking. By eschewing the "do not track" provision discussed above, it allows for a better balancing of consumer and corporate rights and can retain the wealth of information and services currently available to consumers online. The CPBR also allows for the flexibility necessary for the FTC's regulatory scheme to evolve alongside technology, making it an effective solution for the future.

The CPBR establishes a more nuanced form of privacy regulation, one that cannot be summed up as neatly as "do not track." The bill's provisions provide the consumer with a different control over his or her personal information. Under the CPBR regime, the consumer would be able to consent to certain uses of his or her information, while opting-out of other uses.[63] This provision stands in direct contrast to the DNTOA, which only offers the consumer a blanket opt-out.

The default provisions of the CPBR prohibit the use of "covered information by a covered entity for any purpose not authorized by the individual to whom such information relates."[64] The consumer could opt-out of the bill's default provisions, giving a data collector the right to use certain categories of information for behavioral advertising or marketing. At all times, however, the consumer would have to opt-in, via a "clear and conspicuous mechanism," to the collection of sensitive personally identifiable information (including medical conditions and religious affiliation) and to the trans-

---

[62] For an example of a law that seems clumsy in its implementation, consider the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006). Implemented to prevent companies from collecting information from children under the age of 13, *see, e.g.*, *id.* § 6502, its protections can easily be circumvented by an industrious eleven-year old. Most websites, in order to comply, simply require that the user verify their date of birth. Posting of Danah Boyd, *How COPPA Fails Parents, Educators, Youth*, DMLCENTRAL (June 10, 2010, 10:10 AM), http://dmlcentral.net/blog/danah-boyd/how-coppa-fails-parents-educators-youth. It does not take much foresight to realize how simple it would be for a child to falsify that information. *See id.* (noting that "[p]arents teach children to lie about their age to circumvent age limitations"). While the FTC can bring action against those companies that know or have reason to know that children are accessing their website, establishing such knowledge may be difficult, given the prevalence of the drop-down menu as an age verification device. *Id. Cf. An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act: Hearing Before S. Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Sci. & Transp.*, 111th Cong. (2010) (statement of Jessica Rich, Deputy Director of Consumer Protection, Federal Trade Commission), *available at* www.ftc.gov/os/testimony/100429coppastatement.pdf.

[63] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 202 (2011).

[64] *Id.*

fer of previously collected covered information if the transfer "create[d] a risk of economic or physical harm to an individual."[65] Finally, and perhaps most importantly, the consumer would be able to access the information that a company retains about the consumer.[66] The consumer would thereby gain a significant amount of control over his or her personal data without losing the benefits that behavioral advertising brings. Increased consumer control would also subject the data-collecting industries to greater transparency, potentially increasing consumer confidence in doing business online.[67]

While a "do not track" provision seems like a quick fix, the comprehensive protections of the CPBR better protect consumer privacy. The most commonly raised definition of online privacy is the ability to control how one's personal information is collected, stored, and used.[68] Based on the provisions described above, the CPBR would give consumers a more finely tuned tool with which to control data sharing and would allow consumers to correct or change information that has already been collected. The blunt force of the DNTOA offers a much lower level of control.

Furthermore, the CPBR insists on "privacy by design" and "data minimization" tools that will increase consumer confidence in doing business online by ensuring that corporate practices more nearly match consumer expectations.[69] Privacy "cannot be assured solely by compliance with regulatory frameworks;" rather, privacy by design aims to integrate privacy concerns into traditional business models.[70] The Center for Democracy and Technology characterizes privacy by design as a set of seven foundational principles that help businesses comply with fair information practices.[71] Sim-

---

[65] *Id.*; *see also id.* § 3(6) (defining relevant terms).

[66] *Id.* § 202.

[67] At the Commerce, Science, and Transportation Committee hearing, Hewlett Packard ("HP") expressed support for the CPBR on these grounds. Chief Privacy Officer Scott Taylor noted that comprehensive federal privacy legislation will "support business growth, promote innovation and ensure consumer trust in the use of technology." Federal legislation will also "help [HP] compete in the global marketplace since a baseline privacy law in the US allows the opportunity for international interoperability." *Privacy Hearing*, *supra* note 30 (statement of Scott Taylor, President, Sony Network Entertainment International).

[68] *See, e.g.*, Burdon, *supra* note 17, at 69; Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (privacy is "the *control* we have over information about ourselves"); *see also* Kang, *supra* note 55, at 1203. *But see* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821–34 (2000) (critiquing privacy as control paradigm).

[69] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. §§ 103, 301 (2011).

[70] *The Role of Privacy by Design in Protecting Consumer Privacy*, CTR. FOR DEMOCRACY AND TECH. (Jan. 28, 2010), http://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy.

[71] *Id.* The seven foundational principles are (1) Proactive, not Reactive; Preventative, not Remedial; (2) Privacy as the Default; (3) Privacy Embedded Into Design; (4) Full Functionality—Positive Sum, not Zero-Sum; (5) End-to-End Lifecycle Protection; (6) Visibility and Transparency; and (7) Respect for User Privacy. *Id.* Although the CPBR does not explicitly list all seven of these principles, it characterizes privacy by design as "incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals" and "maintaining appropriate management procedures and practices throughout the data life

ilarly, data minimization requires companies to collect only data that is necessary for a given transaction and to retain it for a limited amount of time.[72] Privacy by design and data minimization will require data collectors to behave in a manner more consistent with consumer expectations of privacy; as is, data collectors can freely collect, use, and transfer personal data without consumer knowledge, violating any reasonable definition of privacy.[73]

Finally, the CPBR includes innovative co-regulatory solutions that incorporate the self-regulatory measures that the FTC has previously cultivated in this area.[74] These self-regulatory mechanisms have suffered from difficulties with enforcement and compliance.[75] For example, the Network Advertising Initiative (the "NAI") designated TRUSTe as the third party responsible for enforcing the privacy principles through audits and consumer complaint investigation.[76] But TRUSTe's enforcement was "neither independent nor transparent" and failed to accomplish what it was intended to do.[77]

The co-regulatory portion of the CPBR would designate a third party nongovernmental organization to administer safe harbor programs.[78] However, unlike the self-regulatory setup of the NAI, the FTC would oversee the administering NGO, reviewing its practices and imposing civil penalties if it fails to comply with the CPBR.[79] Today, this kind of symbiotic relationship is commonplace throughout the administrative state, even if not explicitly provided for by implementing legislation.[80] The CPBR is thus not revolutionary in nature, but rather in form, offering a clear directive to take advantage of relationships that already exist in other regulatory contexts.[81]

---

cycle that are designed to ensure that information systems comply with . . . the privacy preferences of individuals." S. 799 § 103. This characterization is consistent with that of the Center for Democracy and Technology.

[72] S. 799 § 301.

[73] *See, e.g.*, Natasha Singer, *Shoppers Who Can't Have Secrets*, N.Y. TIMES, May 2, 2010, at BU5, *available at* http://www.nytimes.com/2010/05/02/business/02stream.html.

[74] These self-regulatory solutions have included, for instance, the Network Advertising Initiative (the "NAI"). The NAI focused exclusively on the network advertising industry and required its members to uphold certain privacy principles. Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 460–61 (2011).

[75] *Id.* at 462.

[76] *Id.*

[77] *Id.* at 463 (quoting PAM DIXON, WORLD PRIVACY FORUM, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION 34 (2007)).

[78] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 501 (2011).

[79] *Id.*

[80] *See* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 547 (2000). Freeman cites several examples of situations in which the government turns to private firms to perform traditional state functions, including contracting out for the delivery of social services such as healthcare, welfare, education, and training. *Id.* at 595.

[81] A co-regulatory solution similar to the CPBR has been enacted in Europe. The European Union's 1995 Data Protection Directive allows each member nation to draft its own data protection statute. Industry representatives then draft a "code of conduct" that embodies the statutory requirements and present it for approval to a regulatory body. If the regulatory body approves the "code of conduct," compliance with the code of conduct is considered compliance with the law. Hirsch, *supra* note 74, at 442.

The CPBR could include further protections for consumers, however. Perhaps the most salient deficiency is the type of information that the bill covers, which is particularly troubling in light of recent concerns about the anonymization of data.[82] Covered information includes personally identifiable information, unique identifier information, as well as "any information that is collected, used, or stored in connection with personally identifiable information or unique identifier information in a manner that may reasonably be used by the party collecting the information to identify a specific individual."[83] Current technology, however, may use uncovered data (e.g., a set of Google searches linked only to an anonymous ID number) in ways that may lead to personal identification.[84] Thus, data that the CPBR defines as preventing the identification of an individual could be used to identify a specific web user.

A 2006 *New York Times* article strikingly illuminates this phenomenon.[85] Two reporters, using a set of publicly available data on the Internet searches of AOL customers, identified and interviewed one of the customers.[86] The customer, a 62-year-old Georgian woman, had searched for "60 single men," "dog that urinates on everything," and "numb fingers."[87] She was identified in the search data only by a seven-digit number and the contents of the searches themselves.[88] An expanded definition of "personally identifying information" that reflects the current technological reality would go a long way toward protecting consumers.

V. Conclusion

The time has come for data privacy legislation in the United States. Passing such legislation will improve the Internet experience for all involved, consumers and the industry alike. The wealth of legislation proposed this session represents Congress's recognition that legislation is essential for the Internet's continued success. When debating different attempts to regulate privacy online, however, Congress must remember that not all bills are created equal and that some offer the possibility of expansive protection for

---

[82] Several authors have suggested that large databases of de-identified data are not safely anonymized, as sophisticated algorithms can connect data points to personally identifiable information. *See* Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 Fordham Intell. Prop. Media & Ent. L.J. 33 (2010); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). *But see* Jane Yakowitz, *Tragedy of the Data Commons,* 25 Harv. J.L. & Tech. (forthcoming 2011) (suggesting that properly de-identified data is safe and should be disseminated as it can have extraordinary social value in the hands of researchers).

[83] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong., § 3(3)(a) (2011).

[84] Gellman, *supra* note 82, at 46.

[85] Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, at A2.

[86] *Id.*

[87] *Id.*

[88] *Id.*

consumers, alongside economic growth. Comprehensive privacy legislation is needed, and the Consumer Protection Bill of Rights offers an excellent starting point.

*—Molly Jennings**

* B.A., Washington University in St. Louis, 2010; J.D. Candidate, Harvard Law School, Class of 2013.