Protecting Privacy in an Era of Weakening Regulation

*Justin Brookman**

We live in a world where every action we take can be observed, recorded, analyzed, and stored. Online, our reading habits are monitored by dozens of faceless companies in order to serve us advertisements.[1] In the physical world, sensors track our smartphones as we walk from store to store,[2] and facial recognition technology is getting better and better at helping businesses recognize their best customers[3] and potential threats.[4] All our personal files are backed up to a remote cloud service, where our private emails[5] or dirty pictures[6] may be illegitimately accessed by malicious hackers.

As tracking technology gets more and more sophisticated, consumers are demanding legal rights over how their information is collected and used. Poll after poll shows that consumers want better consumer protections over personal data.[7] Many mistakenly believe that these protections already exist.

---

* Justin Brookman is Director of Consumer Privacy at the Center for Democracy & Technology where he advocates for stronger privacy protections for personal information. Previously, he served as Chief of the Internet Bureau of the New York Attorney General's office, where he brought consumer protection cases on issues such as data privacy, free expression, and net neutrality.

[1] Jennifer Valentino-Devries & Jeremy Singer-Vine, *They Know What You're Shopping For*, WALL ST. J. (Dec. 7, 2012), http://www.wsj.com/articles/SB10001424127887324784404578143144132736214, http://perma.cc/J8WH-YP69.

[2] Press Release, Senator Al Franken, Sen. Franken Presses Tech Firm to Stop Tracking Consumers Without Their Permission (Mar. 13, 2013), https://perma.cc/GG4T-C6CE.

[3] Brenda Salinas, *High-End Stores Use Facial Recognition to Spot VIPs*, NAT'L PUB. RADIO (July 21, 2013), http://www.npr.org/blogs/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips, http://perma.cc/YM94-3EHS.

[4] Ellen Nakashima, *From Casinos to Counterterrorism*, WASH. POST (Oct. 22, 2007), http://perma.cc/C98M-SNY8.

[5] Amanda Holpuch, *Sony Email Hack: What We've Learned About Greed, Racism, and Sexism*, THE GUARDIAN (Dec. 14, 2014), http://perma.cc/M95T-XPLY.

[6] Brian X. Chen, *Apple Says It Will Add New iCloud Security Measures After Celebrity Hack*, N.Y. TIMES (Sept. 4, 2014), http://perma.cc/X2L7-EWNE.

[7] *See, e.g.*, *GFK Survey of Data Privacy and Trust*, GFK 13 (Apr. 14, 2014), http://perma.cc/B9AP-NNL6 ("[A]lmost 80% of respondents feel that there should be more regulations, preventing organizations from repurposing personal data to third parties. This is a concern across generations."); Mary Madden, *Public Perception of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://perma.cc/M79V-W349 (finding 64% of Americans believe the government should do more to regulate advertisers' privacy practices); JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 23 (2009), http://perma.cc/7MRW-AV9Y; *see also* Data Memorandum from John B. Horrigan, Assoc. Dir., Pew Internet & Am. Life Project, on Use of Cloud Computing Applications and Services (Sept. 2, 2008), http://perma.cc/7FZ8-G94M (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions); Press Release, Harris Interactive, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases When Pri-

One recent study showed that consumers think that the mere existence of a privacy policy on a site means that their personal information is protected.[8] One-third of respondents in another survey, upon hearing conventional behavioral advertising practices described, believed that individuals who engage in those practices should be sent to prison.[9]

Despite growing concern about government surveillance excesses in light of the Edward Snowden disclosures, consumers are even more insistent on the need for stronger limitations on commercial rather than government data collection.[10] For many privacy advocates, this disparity is a bit perplexing: after all, companies don't have the capacity to put you in prison or take away your fundamental freedoms. However, many seem to believe that government surveillance, overbroad or not, is done *for* people (that is, to protect them from terrorism or other threats). Commercial data collection often feels more adversarial: your habits and other activities are tracked in order to get you to buy more stuff. Although many "free" Internet services are fuelled by tracking and advertising, are consumers ultimately being manipulated into spending more money than they otherwise would?[11]

Despite persistent consumer concern about commercial data collection, the legal framework to protect privacy and personal data in the United States is quite weak, both absolutely and especially when compared with the rest of the world. Unfortunately, this is unlikely to be remedied in the foreseeable future; more likely, legal protections in the United States will get still weaker. It will increasingly be incumbent upon Internet users to take action to safeguard their personal information. The good news is that there's a developing market for privacy tools, and in many ways, consumers have the capacity to limit or control what information is collected about them.

In this article, I will briefly describe the state of privacy law in the United States and how its substantive protections are weaker than in other countries. I will then discuss how efforts to improve privacy law have failed in recent years, and likely will continue to fail. Third, I will analyze the ways

---

vacy Safeguards Introduced (April 10, 2008), http://perma.cc/S2TA-QY9Z (announcing a majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests, even when they were told that such advertising supports free services).

[8] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, Pew Research Ctr. (Dec. 4, 2014), http://perma.cc/A7R5-JWZ2 ("Some 52% of internet users believe—incorrectly—that this statement is true, and that privacy policies actually ensure the confidentiality of their personal information."). Companies are required to have a privacy policy by the California Online Privacy Protection Act of 2003. Cal. Bus. & Prof. Code §§ 22575–22579 (West 2014). However, that law does not put any limitations or requirements on what must be contained within a privacy policy; instead, those terms are decided entirely by the company itself.

[9] Joseph Turow et al., *supra* note 7, at 23.

[10] Katherine Jacobsen, *Online Privacy: Americans Worried About Facebook, not NSA, Poll Finds*, Christian Science Monitor (Sept. 5, 2013), http://perma.cc/VKB3-EL39; *Voters Think Google, Facebook Spy More Than Government*, Rasmussen Reports (Nov. 21, 2014), http://perma.cc/QS5Y-MJHR.

[11] *See* John Kenneth Galbraith, The Affluent Society (1958) (arguing that advertising creates artificial demand for products that consumers do not want or need, and that do not offer marginal improvements in quality to other products).

in which privacy protections are actually getting weaker, looking at recent court cases, legislation, and policy frameworks. In conclusion, I will argue that in the face of these weaker legal protections, consumers have an obligation to protect themselves, taking advantage of increasingly powerful services and tools designed with the privacy-conscious in mind. One day, better legal protections must come; in the meantime, consumers have to take the initiative.

I. U.S. Privacy Law Lags Behind The Rest of the World

Most developed nations have comprehensive privacy laws based on the Fair Information Practice Principles[12]—a set of commonly accepted protections that personal information should be afforded. Though there are numerable instantiations of the Fair Information Practices Principles, they all roughly cover the same ground:

- *Transparency*: Companies should be transparent about the personal information they collect.
- *Purpose Specification*: Companies should tell consumers the reasons for which data elements are collected.
- *Use Limitation*: Companies should only use personal data for the reasons disclosed to consumers.
- *Data Minimization*: Companies should only collect the information they need for stated purposes, and should delete data that is no longer necessary for those purposes.
- *Data Accuracy*: Companies should ensure that records maintained about consumers are reasonably accurate.
- *Individual Participation*: Individuals should have access to personal information held by companies, and should have some degree of control over retention and secondary usage of personal information.
- *Security*: Companies should use reasonable protocols to prevent attackers from accessing personal data.
- *Accountability*: Companies (and individuals within those companies) that fail to adhere to the other principles should be held responsible for their actions.[13]

Europe has had comprehensive privacy protections that enshrine these principles into legal requirements since the enactment of the Data Protection

---

[12] David Banisar, National Comprehensive Data Protection/Privacy Laws and Bill 2014 Map (2014), http://perma.cc/W7P2-49HD.

[13] *See* Privacy Policy Guidance Memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. Dep't of Homeland Sec., on The Fair Information Practice Principles: Framework for Privacy Policy at the Dep't of Homeland Sec. (Dec. 29, 2008), http://perma.cc/J3CT-R2C8.

Directive in 1995.[14] Most Latin American and Pacific Rim nations have followed suit.[15] The United States, however, does not have affirmative privacy protections for the vast majority of personal information. Instead, we have a handful of state and federal laws targeted at particularly sensitive data sets (such as information about children,[16] financial information,[17] and health information[18]).

The relatively low baseline privacy protection for all other forms of data in the United States is found in Section Five of the venerable Federal Trade Commission Act (FTCA), a 100-year old consumer protection statute that broadly prohibits companies from engaging in *deceptive or unfair business practices*. Over the last century, the Federal Trade Commission (FTC) has applied the FTCA to a wide range of anti-consumer practices where it can demonstrate that a consumer was deceived, or where a business practice is objectively "unfair" because it (1) causes significant consumer harm that (2) is not avoidable by consumers and (3) is not offset by countervailing benefits.[19] Beginning in 2005, the FTC began bringing actions under the unfairness prong for companies that failed to use reasonable security practices to safeguard personal information.[20] Under the FTC's analysis, poor data security practices meet the statute's three-part test because (1) they lead to exposure of sensitive personal information, (2) they are not detectable or auditable by consumers, and (3) the costs of implementing better policies is far less than the damage done by the poor security practices.[21]

The FTC has also brought a number of cases alleging privacy violations, primarily under the deception prong. During the 2000s, these cases tended to be "gotcha" type cases where the company affirmatively made a clear misstatement in its privacy policy or some other public representation. Under this line of cases, the baseline privacy law in the United States was effectively "don't go out of your way to lie about what you do."[22]

In recent years, the FTC has been more aggressive with its deceptive practices allegations, increasingly arguing that *failure to disclose* surprising

---

[14] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

[15] *International Privacy Laws*, INFORMATION SHIELD, http://perma.cc/4AZJ-QJUH.

[16] Children's Online Privacy Protection Act of 1998 § 1302, 15 U.S.C. §§ 6501–6506 (2012).

[17] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, 6821–6827 (2012).

[18] Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §§ 300gg–300gg-95 (2012).

[19] *See* 15 U.S.C. § 45 (2012).

[20] *E.g.*, BJ's Wholesale Club, Inc., Agreement Containing Consent Order, No. 0423160 (F.T.C. May 17, 2005).

[21] *See* 15 U.S.C. § 45(n) (2012).

[22] *E.g.*, First Amended Complaint for Permanent Injunction and Equitable Relief, F.T.C. v. Toysmart.com LLC, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (alleging deception by breaking promise not to sell personal information in bankruptcy); Complaint, Eli Lilly & Co., 133 F.T.C. 763 (2002) (alleging disclosure of personal information in violation of assurance in privacy policy).

data practices—either in a dedicated privacy policy, or, in some cases, in a more prominent notice—constitutes a material omission, and thus a deceptive practice. For example, the FTC recently alleged that the social network Path committed deceptive practices in failing to meaningfully tell consumers that it was accessing contact information on users' smartphones.[23]

However, there are some elements of the Fair Information Practice Principles that probably cannot be achieved through aggressive enforcement of Section Five. For example, it would be challenging to argue that failure to provide access and correction rights constitutes a deceptive practice (as no one is deceived) or that failure to offer users control of their data is unfair (as no substantial harm is likely to occur, and consumers could avoid any potential harm by merely not using the service). Rather, the FTC has advanced the more limited argument that *if* you decide to offer users control, those controls must work as advertised.[24] As such, despite increased vigilance by the FTC, it does not have the capacity by itself to enshrine all of the Fair Information Practice Principles into U.S. law. For that, Congress must act.

II. Efforts to Improve Legal Privacy Protections Are Failing

Although there is widespread support for greater legal protections around personal data,[25] Congress seems unlikely to enact even very focused pro-privacy legislation in the foreseeable future. As dystopian visions of ubiquitous observation are increasingly made possible, policymakers are apparently unwilling—or unable—to do anything about it.

Legal efforts to address worries around "Big Data" and the proliferation of privacy-invasive technologies are not exactly new. Indeed, the concept of a fundamental legal right to privacy was first articulated in a law review article by future U.S. Supreme Court Justice Louis Brandeis concerned with the proliferation of personal cameras.[26] Brandeis's worry was that cameras in the hands of every citizen would enable the complete surveillance of private citizens; as it turned out, Brandeis's fears were not yet scalable in 1890. However, as data collection and processing becomes increasingly powerful and inexpensive, it seems increasingly likely that Brandeis was merely ahead of his time.

With the rise of computing power in the 1950s and 1960s, concrete concerns about unaccountable credit bureaus led to the initial articulation of the Fair Information Practice Principles (by President Nixon, perhaps ironi-

---

[23] *See* Complaint at 4–5, 8–9, United States v. Path Inc., No. C-13-0448 (N.D. Cal. Jan. 31, 2013).

[24] *See* Complaint, *In re* Chitika, Inc., No. C-4324 (F.T.C. June 17, 2011). For further analysis of the FTC's privacy enforcement under Section five, *see* Woodrow Harzong & Daniel Solove, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).

[25] *See* GFK, *supra* note 7, at 6.

[26] Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

cally)[27] and the enactment of the Fair Credit Reporting Act (FCRA) to give individuals the right to access and fix inaccurate personal records that could be used to deny consumers credit or employment.[28]

A. Efforts to Update Statutory Privacy Law Are Failing

The next wave of consumer privacy concerns derived from the emergence of the Internet in the 1990s, as consumers began to be aware of the potential for unprecedented data collection about their personal habits. Third-party advertising companies developed the capacity to build detailed profiles about the websites consumers visited despite having no relationship with them whatsoever. Senator Fritz Hollings introduced the Online Personal Privacy Act to give consumers more control over personal information,[29] but the bill failed to advance.[30] Moreover, momentum for a new law was already imperiled by the election of a new anti-regulatory president in 2000, and the terrorist attacks of 9/11 meant that privacy would be a backburner issue for several years.

Eventually, policymakers began again to acknowledge consumer dissatisfaction with the lack of consumer privacy protections. Starting in 2010, Congress began to seriously consider again the idea of passing comprehensive privacy legislation. Representatives Rick Boucher and Bobby Rush both introduced comprehensive privacy bills that year that would pertain to all personal information; despite a hearing, neither bill was marked up or voted out of Committee.[31] The following year, Senators Kerry and McCain introduced a bipartisan bill in the Senate, though again, no vote was ever taken.[32] In 2012, the FTC for the first time called for comprehensive privacy legislation; previously, the agency had taken the position that its existing consumer protection authority was sufficient to protect individual privacy.[33] That same year, the White House also for the first time called for comprehensive pri-

---

[27] *See* U.S. Dep't of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records Computers and the Rights of Citizens (1973). For more on the history of the development of the Fair Information Practice Principles, *see generally* Robert Gellman, *Fair Information Practices: A Basic History* (Feb. 11, 2015), http://perma.cc/6UJZ-4QAE.

[28] Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 602-629, §§ 1681–1681x (2012).

[29] 148 Cong. Rec. S2, 957–59 (daily ed. Apr. 18, 2002) (statement of Sen. Ernest Hollings).

[30] *S. 2201 (107th): Online Personal Privacy Act, History*, GovTrack, https://perma.cc/5TW9-UW2U.

[31] *The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation: Hearing on H.R. 5777 Before the H. Comm. on Energy and Commerce and H. Subcomm. on Commerce, Trade and Cons. Protection*, 111th Cong. (2010) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy and Technology).

[32] *S. 799 (112th): Commercial Privacy Bill of Rights Act of 2011*, *History*, GovTrack, https://perma.cc/XQ4P-8QCU.

[33] The FTC reiterated this demand in its final version of the privacy report. *See* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, iv-v, 11–14 (2012), https://perma.cc/6FHR-JL3Y.

vacy legislation to address the growing wave of unchecked and unaccountable data collection.[34]

Unfortunately, given the extremely partisan nature of policy debates in Washington, the President's full-throated endorsement of privacy legislation was probably its death knell for the foreseeable future. Republicans increasingly pointed to potential privacy regulations as a threat to the burgeoning data-driven economy.[35] The House Subcommittee on Commerce, Manufacturing, and Trade held a hearing tellingly titled "Internet Privacy: The Impact and Burden of EU Regulation," indicating that similar mandatory privacy requirements on businesses were unlikely to advance in that chamber anytime soon.[36] President Obama eventually released a draft privacy bill in February 2015 (three years after calling for such legislation). While the bill had clearly been crafted to account for industry concerns about overregulation—so much so that many roundly criticized the bill as too weak[37]—the bill has widely been recognized as dead on arrival.[38]

Other, more modest legislative efforts designed to improve consumer privacy in recent years have met similar fates. In 2012, Senator Al Franken introduced the Location Privacy Protection Act (LPPA) to require companies to only use precise geolocation information with the consent of the consumer.[39] While the bill passed out of the Judiciary Committee in December of that year, it advanced no further. At least the LPPA got a vote—in the past three Congresses, no other bill to increase commercial legal privacy protections even made it out of committee in either the House or Senate.

---

[34] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), http://perma.cc/CS4D-8KKJ.

[35] *See, e.g.*, Press Release, U.S. Congressman Marsha Blackburn, Blackburn Responds to White House Privacy Report (Feb. 23, 2012), https://perma.cc/LJG4-C72C (warning that "big government" regulation of privacy could lead to "unintended consequences that will end up costing American jobs").

[36] *Internet Privacy: The Impact and Burden of EU Regulation: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy and Commerce*, 112th Cong. (2011).

[37] *See* Tracey Lien, *Consumer Privacy Bill of Rights Doesn't Go Far Enough, Critics Say*, L.A. Times (Mar. 3, 2015), http://perma.cc/7FY3-4794; *see also* Ctr. for Democracy and Tech., *Analysis of the Consumer Privacy Bill of Rights Act* (Mar. 2, 2015), https://perma.cc/UVN9-E2QG; The Editorial Board, *The President's Weak Privacy Proposal*, N.Y. Times, Mar. 6, 2015, at A28.

[38] Elizabeth Spainhour, *FTC Commissioner Comments on Consumer Privacy Bill of Rights*, Digital Media & Data Privacy Law Blog (Mar. 9, 2015), https://perma.cc/H65B-CK7Z (citing FTC Commissioner Brill as admitting passage of the bill was "unlikely given other legislative priorities at this time").

[39] Location Privacy Protection Act of 2012, S.1223, 112th Cong. (2012). Cell carriers already operate under similar restrictions today under the Telecommunications Act of 1996 and Cable Communications Policy Act of 1984. *See Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech., and the Law*, 112th Cong. (statement of Justin Brookman, Director, Consumer Privacy, Center for Democracy and Technology).

B. Without Legislative Pressure, Self-Regulatory Efforts Fail As Well

In the absence of advances in legislation, industry efforts to voluntarily self-regulate have also cratered. Predictably, self-regulatory efforts follow a standard trend: once interest in legislation perks up on Capitol Hill, industry scrambles to demonstrate its own capacity to address the problem itself. Once Congress's attention has waned or turned to other matters, however, industry momentum toward meaningful rules often falls by the wayside.

In privacy, this cycle has happened before. As discussed above, the late '90s and early 2000s saw the last serious effort to pass data privacy legislation prior to recent years. The online advertising industry—which had felt the brunt of privacy pressure in the preceding years—promised to voluntarily agree to stringent privacy rules in lieu of new legislation. In response to an FTC investigation into behavioral advertising practices, the leading advertising companies announced the formation of the Network Advertising Initiative (NAI) to develop a strong self-regulatory code that would limit how advertising data could be used, and offer consumers meaningful choices about the use of their data for advertising.[40] However, once regulatory pressure eased, NAI was slow to put forward these rules and opaque about how those rules were being developed; when a code was finally announced, privacy advocates lambasted the rules as wholly insufficient.[41] Companies increasingly felt unwilling to follow even these rules; NAI began accepting "associate" members who paid dues but didn't agree to follow the NAI code.[42] Indeed, within a few years, only two companies voluntarily complied with the NAI's guidelines.[43] In any event, it is clear that this effort has done little to address consumer unease with online behavioral advertising.[44]

More recently, when the Obama administration announced support for comprehensive privacy legislation in 2012, the leading industry trade associations committed to improving self-regulatory efforts; most notably, they agreed to voluntarily honor the "Do Not Track" flags that major Internet browsers had allowed users to set starting in 2011.[45] The Internet standards body World Wide Web Consortium ("W3C") set out to define the

---

[40] Press Release, Fed. Trade Comm'n, Federal Trade Commission Issues Report on Online Profiling: Commends Network Advertising Initiative's Self-Regulatory Principles (July 27, 2000), https://perma.cc/V9XR-4M4W.

[41] Electronic Privacy Info. Ctr., *Network Advertising Initiative: Principles Not Privacy*, EPIC.ORG (July 2000), https://perma.cc/8UCH-VBKC.

[42] Pam Dixon, *THE NETWORKING ADVERTISING INITIATIVE: Failing at Consumer Protection and at Self-Regulation,* WORLD PRIVACY FORUM (Nov. 2, 2007), https://perma.cc/BN2N-H3WA.

[43] *Id.*

[44] *See* GFK, *supra* note 7, at 6.

[45] Danny Weitzner, *We Can't Wait: Obama Administration Calls for a Consumer Privacy Bill of Rights for the Digital Age*, WHITE HOUSE BLOG (Feb. 23, 2012), https://perma.cc/9L7C-5MFX. Do Not Track signals are headers attached to web requests sent by your browser when fetching a page. The header indicates that the user has indicated a preference not to be tracked from site to site; however, this preference is probably not legally binding, at least in the United States.

parameters and syntax of the Do Not Track signal. Initially, the advertising industry participated heavily in the development of the standards, and many voluntarily limited data collection and usage in response to the signals.[46] Over time, however, as the momentum for legislation and other regulatory threats ebbed, the ad industry lost interest and largely pulled out of the process.[47] Currently, only a handful of Internet companies such as Twitter and Pinterest do anything at all in response to consumers' Do Not Track signals.[48]

Even self-regulatory efforts specifically convened by the White House have foundered. At the same 2012 event where the administration announced support for privacy legislation and an industry commitment to honor Do Not Track, the White House stated that it would convene multi-stakeholder processes designed to come up with voluntary industry codes that could be enforced by the FTC if adopted.[49]

The Obama administration's first self-regulatory convening focused on mobile transparency: how to meaningfully convey on a small screen what sort of personal information is being collected by the apps on your smartphone. The initial meeting of this effort drew hundreds of participants who debated no less than sixty separate proposals.[50] However, over time, the process got bogged down in minutiae, and fewer and fewer participants were willing to engage in negotiations. By June 2013, a code was hammered out by a small group of remaining participants, but usability experts, and even the FTC, criticized it.[51] A handful of companies—most notably Intuit—agreed to use the group's transparency best practices,[52] but by and large the principles have been ignored by industry. Last year, the administration announced a second multi-stakeholder effort to hammer out best practices for

---

[46] Joshua Fairfield, *Do-Not-Track As Default*, 11 NW. J. TECH. & INTELL. PROP. 575, 582 (2013).

[47] *Id.*

[48] While Twitter and Pinterest do not operate large ad networks that display content on a wide range of other sites, they do allow websites to embed sharing widgets. Thus, a site publisher like NYTimes.com can embed a Twitter sharing widget that triggers a call to Twitter to render the widget whenever a page is loaded. Millions of pages around the web include such widgets, allowing the companies that serve them to recognize cookies previously placed to track you around the internet — whether you click on those widgets or not. However, Twitter and Pinterest have promised to limit data collection and use for data collected in generating widgets when users turn on Do Not Track. *E.g.*, *Twitter Supports Do Not Track*, TWITTER (2014) https://perma.cc/HX89-Y448.

[49] *See* 15 U.S.C. 45(a)(1). The FTC would have jurisdiction over such codes because a statement of adherence to a code would be a consumer representation; if a company ended up violating such a statement, that would constitute a deceptive business practice under the law.

[50] Kristin Shaffer, *Recapping the NTIA Multistakeholder Meeting*, INSIDE PRIVACY: UPDATES ON DEVELOPMENTS IN GLOBAL PRIVACY & DATA SECURITY FROM COVINGTON & BURLING (July 13, 2012), https://perma.cc/58HR-PRR3.

[51] Grant Gross, *A Federal Push for Mobile Privacy Has Failed, Critics Say*, PC WORLD (Aug. 29, 2013), https://perma.cc/QH5B-T2G8.

[52] *Intuit Supports NTIA Code of Conduct for Mobile App Transparency*, INTUIT (July 29, 2013), http://perma.cc/W2M4-3NJT.

facial recognition technologies. Several months later, interest and participation in the group has waned significantly, and no code has been introduced.[53]

III. Privacy Law Isn't Just Stalled, It's Going Backwards

At the same time that various efforts to advance privacy law are stuck in a quagmire, other recent trends, including the rising protections for corporate speech[54] paired with growing resistance to putting transparency or any other regulatory requirements on companies,[55] are chipping away at the United States's already weak existing privacy framework. Rather than working to extend existing privacy protections, policymakers are on several fronts rolling back existing rights. These attacks are taking place in a number of places, including the courts, Congress, and administrative and industry policy guidance.

A. Chipping Away at Privacy in the Courts

One avenue of attack on existing privacy law is the First Amendment. Some companies are increasingly making the argument that because privacy laws by their nature are limitations on the collection and dissemination of information, they fall afoul of the First Amendment's prohibition on laws abridging the freedom of speech.

This notion was upheld by the Supreme Court in *Sorrell v. IMS Health Inc.*[56] In that case, the Supreme Court overturned a Vermont law that prohibited pharmaceutical companies from accessing doctors' prescribing records for the purpose of determining how to market to those doctors. The Court held in a 6-3 opinion that the Vermont statute violated pharmaceutical companies' free expression rights—not because they were limited in what they could say, or to whom, but because they were deprived of the underlying data with which they could better target their message. After *Sorrell*, any privacy restriction specifically aimed at marketing uses of data will be suspect. Taken to its extreme, however, the *Sorrell* holding could be used to argue against any limitation of access to personal information (let alone use).

This free speech defense to violation of privacy laws has been used in other cases as well. In *King v. General Information Services, Inc.*, a data broker argued that the FCRA violated the First Amendment because it prohibited credit reports from including information on debts over seven years old.[57] The defendant's argument was that the fact of the older debt was truth-

---

[53] *See Privacy Multistakeholder Process: Facial Recognition Technology*, National Telecommunications & Information Administration (2014), http://perma.cc/KLS9-PNKS.

[54] *See generally* Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010) (holding that the government may not suppress free speech on the basis of the speaker's corporate identity).

[55] *See* discussion *infra* Part II.A.

[56] 131 S. Ct. 2653 (2011).

[57] 903 F. Supp. 2d 303 (E.D. Pa. 2012).

ful information, and FCRA amounted to a government restriction on his expression of that fact. General Information Services was not successful on its motion to dismiss,[58] and the case was ultimately settled out of court.[59] Notwithstanding this case, courts have in other instances struck down longstanding privacy laws on free expression grounds. In Texas, for example, a court invalidated the state's peeping Tom laws on the grounds that the law prohibited the collection of personal (if highly private and sensitive) images in violation of the First Amendment.[60] If the collection of any truthful information (no matter how personal) is broadly protected on free expression grounds, companies may have wide latitude to collect *any* information about us without fear of statutory prohibition. In an era of lessening distinctions between the press and private citizens, and between private citizens and companies, will courts continue to recognize a difference between the data collection practices of *The New York Times* and a commercial data broker that sells information to better target marketing?

Another avenue where the courts are chipping away at existing privacy protection is through narrowing the concept of Article III standing. As some have sought to reframe informational privacy as a prevention of concrete harms instead of the ability to control what information others can collect about you,[61] many court cases have challenged the notion that the *mere observation of facts* qualifies as an injury sufficient to meet the "case or controversy" requirement necessary for standing before the courts.[62]

Thus, courts have rejected a number of cases alleging privacy violations because the complaints have not asserted a cognizable injury to consumers stemming from a violation of privacy.[63] Courts have routinely rejected arguments that companies' collection of personal information for advertising (or other) purposes deprives consumers of any monetary benefit; embarrassment or conjectural fear of identity theft has been found to be insufficient to confer standing.[64] The Ninth Circuit has taken a more expansive view of standing; in effect, it has said that if Congress confers onto consumers a cause of action for violation of a statutory right, that is sufficient for jurisdiction.[65] The Supreme Court had been poised to address this split a couple of years ago in the *First American v. Edwards* case.[66] In that case, a federal statute

---

[58] *Id.* at 313 (E.D. Pa. 2012).

[59] Press Release, Gen. Info. Servs., Gen. Info. Servs. Announces Settlement of King v. GIS and Dowell v. GIS (June 2014), *available at* https://perma.cc/Y37W-BDZJ.

[60] *Ex parte* Thompson, 442 S.W.3d 325, 350 (Tex. Crim. App. 2014); *see also* U.S. West Inc. v. Fed. Comm. Comm'n, 182 F.3d 1224, 1248 (10th Cir. 1999) (vacating FCC rules that limited carrier use of customer communications records for marketing purposes).

[61] *See* discussion *infra* Part III.C.

[62] *E.g.*, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); LaCourt v. Specific Media, Inc., No. SACV 10–1256–GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011).

[63] *See, e.g.*, *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *13 (N.D. Cal. Dec. 3, 2013).

[64] *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434 (D. Del. 2013); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1032 (N.D. Cal. 2012); *In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14 (D.D.C. 2014).

[65] *See, e.g.*, Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 793 (N.D. Cal. 2011).

[66] 132 S. Ct. 2536 (2012).

granted consumers the right to sue for liquidated damages for title insurance impropriety; however, in Ohio, title insurance rates are prescribed by statute, so there was no argument that consumers were harmed in any way by the impropriety. First American's petition for certiorari was granted; however, the Supreme Court subsequently reversed course, curiously dismissing the case on the grounds that cert had been "improvidently granted."[67]

Nonetheless, companies are continuing to argue that Article III requires a showing of demonstrable harm before a court can adjudicate an alleged privacy violation. Recently, the data broker Spokeo appealed a Ninth Circuit determination that consumers have standing to bring an allegation under the Fair Credit Reporting Act for inaccurate credit reports absent a showing that they had been harmed as a result.[68] In support of this petition, internet giants Facebook, Google, Yahoo!, and eBay filed an *amicus* brief arguing that the Supreme Court should take the case, since they had been subjected to numerous, expensive lawsuits over alleged privacy violations that resulted in no tangible harms.[69]

Companies are also increasingly using the courts to challenge the FTC's use of the FTCA to enforce against privacy and security violations. Despite ten years' worth of enforcement actions against companies for unreasonable data security practices under Section Five's unfairness authority,[70] this authority is currently being challenged in two separate court cases. In *Wyndham v. Federal Trade Commission*,[71] the hotel conglomerate argued that Section Five's prohibition on unfair business practices does not extend to the objectively poor data security practices it employed to protect sensitive consumer data such as credit card and other financial data.[72] Similarly, in the FTC's enforcement action against LabMD, a medical office company is arguing that the prohibition on unfairness does not prohibit a company from installing public file-sharing software on a computer that stores unencrypted medical records—again, an objectively absurd data security practice.[73] It remains to be seen whether these legal arguments will be successful; nevertheless, these cases are exacting a significant toll on the FTC's legal resources, limiting its ability to bring new enforcement actions.

---

[67] *Id*. at 2537 (dismissing certiorari as improvidently granted).

[68] *See* Robins v. Spokeo, Inc., 742 F.3d 409, 410–11 (9th Cir. 2014); *see also* Brief for Petitioner, Spokeo, Inc. v. Robins, No. 13-1339 (filed May 7, 2014).

[69] Brief for Amici Curiae eBay Inc., Facebook Inc., Google Inc., and Yahoo! Inc. in Support of Petitioner at 4, Spokeo, Inc. v. Robins, No. 13-1339 (filed June 6, 2014). The Supreme Court granted Spokeo's petition for *certiorari* on April 27. Spokeo, Inc. v. Robins, 135 S. Ct. 1892 (2015) (order granting certiorari).

[70] *See supra,* Section I; Federal Trade Commission, 2014 Privacy and Data Security Update (2015), https://perma.cc/HJ8R-C2AN.

[71] 10 F. Supp. 3d 602 (D.N.J. 2014).

[72] *See id.* at 607; *see also* Appellant's Opening Brief and Joint Appendix Vol. 1 at 47, Fed. Trade Comm'n v. Wyndham Worldwide Corp. (No. 14-3514) (filed Oct. 6, 2014).

[73] *See* Complaint at 5; *In re* LabMD, No. 9357 (F.T.C. Aug. 29, 2013); Resp't LabMD Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings at 9, 14, *In re* LabMD, No. 9357 (F.T.C. Nov. 12, 2013).

B. Watering Down Existing Legal Protections in Congress

In addition to the legal challenges, Congress is looking askance at the FTC for its enforcement actions on privacy and security. In July of last year, the House Oversight and Government Reform Committee held a hearing investigating whether the agency has overstepped its authority in cases like *Wyndham* and *LabMD* (no one from the FTC itself was invited to testify). During the hearing, Chairman Darrell Issa repeatedly lambasted the agency for regulatory overreach, accusing the FTC of engaging in "erroneous inquisitions" in its pursuit of data security.[74]

As discussed above, Congress has failed to make meaningful progress on statutory data privacy reform in recent years; the most recent law enacting substantive improvements to privacy protections was the Health Information Technology for Economic and Clinical Health (HITECH) Act from the previous decade.[75] On the other hand, legislation to *weaken* existing privacy laws has been, and likely will continue to be, more successful. In 2013, Congress passed the Video Privacy Protection Act Amendments of 2012, which made the consent requirements for the sharing of video-watching records (one of the few categories of data with affirmative statutory protections)[76] somewhat less stringent.[77]

For the next Congress, observers generally agree that the most likely commercial privacy or security legislation to advance will be data breach notification legislation.[78] Such a law would require that companies that lose especially sensitive data (such as financial account passwords or Social Security numbers) in a data breach to notify consumers of the incident, putting them on notice that their accounts may be illegitimately accessed.[79] Already, forty-seven states (as well as the District of Columbia, Puerto Rico, and most federal territories) have data breach notification requirements; however, the requirements vary slightly from jurisdiction to jurisdiction.[80] Federal law would broadly preempt the states, and replace their requirements with a uniform standard.[81]

---

[74] Julian Hattem, *Rep. Issa Takes Aim at FTC 'Inquisitions,'* THE HILL (July 24, 2014), http://perma.cc/DWM6-2RPU.

[75] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 226.

[76] 18 U.S.C. § 2710 (2012). The Video Privacy Protection Act was passed in 1988 after an investigative reporter obtained the video renting records of Supreme Court nominee Robert Bork during his confirmation process. *See* Andrea Peterson, *How a Failed Supreme Court Bid is Still Causing Headaches for Hulu and Netflix*, WASH. POST (Dec. 27, 2013), http://perma.cc/C2G8-YXXK. The law generally requires affirmative consent before a service provider can share information about video watching with third parties.

[77] Justin Brookman, *House Tweaks Video Privacy Law for Frictionless Sharing*, CDT BLOG (Dec. 7, 2011), https://perma.cc/2WSG-ZHXC/.

[78] *See, e.g.*, Cory Bennett, *Lawmakers See Momentum for Data Breach Legislation*, THE HILL (Jan. 27, 2015), http://perma.cc/45YX-PRDA.

[79] *Id.*

[80] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://perma.cc/K2ZW-2EHQ.

[81] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

And therein lies the problem: Congress is trying to address the one substantive area where most states have already legislated strong protections. At best, a uniform federal law (without additional substantive protections) would simply make it less complicated for companies that experience a data breach incident by simplifying the legally mandated response. The hassle and expense of data breach notification is a feature of these laws, not a bug, since they incentivize companies against using poor data security. Simply streamlining the process reduces this incentive. A federal bill might also stop the states from expanding on their existing protections; for example, states like California and Florida have recently broadened the scope of their breach notification bills beyond financial data to any illegitimate account access.[82]

That, of course, is the *best case* for a federal breach notification law, absent some new consumer protection element.[83] On the other hand, federal legislation could be substantially weaker than existing standards, and could broadly preempt the states from enacting additional data protection measures. Unfortunately, this is what most proposed bills accomplish. None of the bills that have been proposed in the current Congress are as strong as the existing laws in states like California and New York; most are substantially weaker, and would allow companies to evade breach notification in many instances where they must notify consumers of breaches under the existing law.[84] All would preempt state data breach laws, prohibiting states from requiring their own form of breach notification, and in some cases preventing states from enacting notification requirements for other forms of data not addressed by the federal bill, or from passing any other protections on privacy, security, or data protection. A bill proposed by President Obama earlier this year is better than many of the Congressional proposals, but still has overly broad preemption language and weaker enforcement powers than many existing state laws.[85]

---

[82] Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82 (Deering 2014); Fla. Stat. Ann. § 501.171 (LexisNexis 2014).

[83] Early versions of federal breach notification bills often included data broker access requirements that would afford consumers a statutory right to view and correct files about them held by third party data brokers. *See The Data Accountability and Trust Act and the Informed P2P User Act: Hearing on H.R. 2221 and H.R. 1319 Before the H. Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. 1 (2009) (statement of David Sohn, Senior Policy Counsel, Center for Democracy and Technology).

[84] *See*, *e.g.*, Meena Harris, *Comparison of Five Data-Breach Bills Currently Pending in the Senate*, Inside Privacy: Updates on Developments in Global Privacy & Data Security From Covington & Burling (Feb. 24, 2014), http://perma.cc/B9DJ-YL92.

[85] Seventeen state laws today allow for a private right of action in the event of a data breach. *See Data Breach Charts*, BakerHostetler, http://perma.cc/RR8C-N49K. The President's proposed legislation only allows for regulator enforcement and preempts state remedies. It also would preempt state notification laws covering categories of data not addressed by the federal law. *See* G.S. Hans, *White House Data Breach Legislation Must Be Augmented to Improve Consumer Protection*, CDT Blog (Jan. 16, 2015), https://perma.cc/G62Y-SBF2.

C. Policy Pushback: Even Fair Information Practice Principles Are Under Attack

In recent years, we have even seen efforts to literally *redefine* the concept of privacy in ways that weaken individual self-determination and minimize concerns about data collection. Thus, some have argued that privacy is no longer defined in terms of user self-determination, but in terms of trusting companies to make the right decisions with regard to whatever data they decide to collect about you. This narrative holds that the potential societal benefits of Big Data are so vast that traditional privacy principles such as data minimization, individual control, and use limitation no longer make sense in the modern world. Rather, privacy should now primarily be about protecting consumers from harmful uses of their personal information. Some have criticized this shift from individual autonomy to corporate responsibility as "data paternalism";[86] nevertheless, efforts to promote this vision have dramatically escalated in just the past couple of years.[87]

In February 2013, the World Economic Forum released the paper, "Unlocking the Value of Personal Data: From Collection to Usage." As indicated by the title, the primary conclusion of this paper is that laws and regulations need to shift to address the *use* of personal data, rather than the underlying collection, transfer, or retention.[88] Others have echoed the same theme: As Viktor Mayer-Schönberger, a leading proponent of this view bluntly put it, "[t]he naked truth is that informational self-determination has turned into a formality devoid of meaning and import."[89] This argument is based in part on the premise that companies can get consumers to consent to *anything* by putting requirements into an opaque terms of service agreement they will never read. While some might argue that the failure of privacy policies and boilerplate license agreements is evidence of a need for clearer and more prominent privacy notices, others seem to take the lesson that consumer control of personal information simply doesn't matter anymore.[90]

As extreme as this notion sounds, it has found some purchase in policymaking circles. Last year, the Obama administration conducted a "Big Data" review in order to assess whether the traditional Fair Information Practice Principles still matter in the era of Big Data. The final report, authored by longtime Democratic operative John Podesta, was a sober and de-

---

[86] *See, e.g.*, ANN CAVOUKIAN ET AL., INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, THE UNINTENDED CONSEQUENCES OF PRIVACY PATERNALISM 15 (2014), *available at* https://perma.cc/5B6M-9Z4C.

[87] *See, e.g.*, Benjamin Wittes & Wells C. Bennett, *Databuse and a Trusteeship Model of Consumer Protection in the Big Data Era*, BROOKINGS INSTITUTE (June 2014), http://perma.cc/TE3W-WNCJ.

[88] WORLD ECONOMIC FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 11–13 (2013), http://perma.cc/GTE9-8U4Y.

[89] Eduardo Ustaran, *Yes, Consent Is Dead. Further, Continuing To Give It a Central Role Is Dangerous*, IAPP PRIVACY PERSPECTIVES BLOG (Dec. 18, 2013), https://perma.cc/R8Q5-SSFS.

[90] *See id.*

scriptive analysis of the potential benefits and privacy costs of Big Data that mostly reserved judgment on the hardest policy questions posed by the advances in surveillance and analytical technologies.[91]

At the same time, however, a parallel Big Data report was released by the President's Council of Advisors on Science and Technology (PCAST)—an official advisory group of external experts.[92] This report struck a markedly different tone than the Podesta report. The PCAST report embraced many of these same ideas about the inevitability of all data collection and the futility of data minimization; the report tendentiously argued that since tactics such as data deletion and data de-identification can in some circumstances be reversed engineered, they should not be relied upon at all. Deletion and minimization (in addition to collection limitations) are core aspects of data minimization, which has been a key Fair Information Principle for decades; the PCAST review casually argues that because those techniques may in some scenarios be imperfect, they should be disregarded altogether.[93]

Alarmingly, the report seems to enthusiastically embrace a dystopian world where companies and governments surveil every aspect of our lives, without at all countenancing the potential pitfalls (such as data breach or government abuse) associated with unlimited personal surveillance.[94] The report offered the following case as an example of why we should give up our previously held notions of commercial privacy and embrace Big Data:

> Taylor Rodriguez prepares for a short business trip. She packed a bag the night before and put it outside the front door of her home for pickup. No worries that it will be stolen: The camera on the streetlight was watching it; and, in any case, almost every item has a tiny RFID tag. Any would-be thief would be tracked and arrested within minutes. Nor is there any need to give explicit instructions to the delivery company, because the cloud knows Taylor's itinerary and plans; the bag is picked up overnight and will be in Taylor's destination hotel room by the time of the arrival.
>
> Taylor finishes breakfast and steps out the front door. Knowing the schedule, the cloud has provided a self-driving car, waiting at the rub. At the airport, Taylor walks directly to the gate—no need to go through any security. Nor are there any formalities at the gate: A twenty-minute "open door" interval is provided for passengers to stroll onto the plane and take their seats (which each sees individually highlighted in his or her wearable optical device). There

---

[91] White House, Big Data: Seizing Opportunities, Preserving Values (2014), http://perma.cc/8VPX-DB8E.

[92] President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective (May 2014), http://perma.cc/WQ8H-B5ZK.

[93] *See id.*

[94] *See* Justin Brookman and G.S. Hans, Why Collection Matters: Surveillance as a De Facto Privacy Harm (2013), http://perma.cc/M77Z-3TNN.

> are no boarding passes and no organized lines. Why bother, when Taylor's identity (as for everyone else who enters the airport) has been tracked and is known absolutely? When her known information emanations (phone, RFID tags in clothes, facial recognition, gait, emotional state) are known to the cloud, vetted, and essentially unforgeable? When, in the unlikely event Taylor has become deranged and dangerous, many detectable signs would already have been tracked, detected, and acted on?
>
> Indeed, everything that Taylor carries has been screened far more effectively than any rushed airport search today. Friendly cameras in every LED lighting fixture in Taylor's house have watched her dress and pack, as they do every day. Normally these data would be used only by Taylor's personal digital assistants, perhaps to offer reminders or fashion advice. As a condition of using the airport transit system, however, Taylor has authorized the use of the data for ensuring airport security.
>
> Taylor's world seems creepy to us. Taylor has accepted a different balance among the public goods of convenience, privacy, and security than would most people today. Taylor acts in the unconscious belief (whether justified or not, depending on the nature and effectiveness of policies in force) that the cloud and its robotic servants are trustworthy in matters of personal privacy. In such a world, major improvements in the convenience and security of everyday life become possible.[95]

It is quite striking to see such a stark critique of the fundamental value of privacy in an official government report—even one from a technical advisory group. While this perspective has not been wholly endorsed by the Administration, elements of this worldview are evident in the President's proposed Consumer Privacy Bill of Rights.[96] Only time will tell if subsequent policy guidance from future administrations will continue down the road of discounting privacy in favor of convenience and security.

IV. Absent Legal Protections, Consumers Must Demand Privacy Controls and Protections from the Services They Use

Government reports aside, it is clear that Americans have not by and large adopted the opinion that privacy is unimportant. Many of us feel a nagging sense that our privacy is increasingly being violated, and consumers feel that this means more needs to be done to ensure personal privacy, not

---

[95] President's Council of Advisors on Science and Technology, *supra* note 92, at 17–18.

[96] *See* Ctr. for Democracy and Tech, *supra* note 37.

less.[97] With policy lagging, it will increasingly be incumbent upon individuals to push back on notions of data paternalism, and take steps to control the dissemination and collection of their personal information.

Efforts to improve consumer legal protections—at least at the federal level—are unlikely to be successful in the short to medium-term. At this point, privacy advocates are mostly playing defense to stop the erosion of existing privacy protections. While it may be possible to enact marginal protections at the state level,[98] states are limited in how much they can accomplish: because of the seamless nature of the Internet, state efforts to comprehensively regulate online privacy are likely to run afoul of the Commerce Clause.[99]

In the meantime, it will increasingly be incumbent upon consumers to use self-help to protect their privacy, and to choose services based on privacy practices. Unfortunately, this is fairly challenging today; many consumers have a vague sense that their privacy is being violated, but they don't really know how. By and large, privacy policies aren't helpful for evaluating actual privacy practices. Consumers don't have the time to parse through a 10,000-word legal document for every webpage they visit,[100] and privacy policies often don't contain precise information about what companies actually do with your data. Because privacy enforcement in the United States has historically been limited to affirmative misstatements, companies tend to draft extremely vague privacy policies that reserve broad rights over how they may use and transfer personal information, typically going well beyond what they actually do with that information.

Fortunately, however, some companies are starting to feel market pressure to prominently assure consumers that certain data collection or usage is off limits. Fitbit, the company that makes wearable fitness gear, recently promised its users that it would not sell sensitive health information to third-party data brokers;[101] Apple is requiring the same promises from application developers as a condition of gaining access to the iTunes Store.[102] Increasingly, many services are being marketed with privacy and information con-

---

[97] *See* Mary Madden, *supra* note 7.

[98] *See* discussion of state data breach notification laws *supra* Part III.B.

[99] *See*, *e.g.*, American Library Association v. Pataki, 969 F. Supp. 160, 167, 173–77 (S.D.N.Y. 1997) (holding that the Internet fits within the parameters of interests traditionally protected by the Commerce Clause).

[100] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 565 (2009) (estimating that consumers would need to spend approximately 201 hours per year to actually read website privacy policies, at a collective national cost of $781 billion per year).

[101] Fitbit Privacy Policy, Fitbit, http://perma.cc/2L7U-RSJM ("First and foremost: We don't sell any data that could identify you. We only share data about you when it is necessary to provide the Fitbit Service, when the data is de-identified and aggregated, or when you direct us to share it."); Niels Lesnewski, *Schumer Praises New FitBit Privacy Policy*, Roll Call (Aug. 22, 2014), http://perma.cc/G47V-3W8F.

[102] Mark Sullivan, *Apple Prohibits HealthKit App Developers From Selling Health Data*, VentureBeat (Aug. 28, 2014), http://perma.cc/MZ5F-WHPS.

trol as a key feature: Snapchat, Whisper, and WhatsApp have all experienced rapid growth due to customer demand for communications platforms that leak less personal data.[103] Indeed, online encryption protection—rare even two years ago apart from e-commerce sites that collected financial information—is increasingly becoming the standard for general-purpose sites.[104] While encryption only limits outside attacker access to personal information—not the sites you visit or their business partners—the marked increase in the use of encryption does denote a market response to consumer anxieties about online privacy.

Independent evaluators are increasingly assessing large service providers based on how they use and protect personal information. For the past two years, for example, the Electronic Frontier Foundation (EFF) has published "Who Has Your Back?," a multifactor rating of how major internet companies respond to government requests for access to personal information.[105] EFF has also published comparisons of the various private messaging platforms that have sprung up in response to consumer demand.[106]

Third-party service providers are also popping up to help manage consumers' privacy at scale for other companies. For example, Catalog Choice is a popular service that allows people to opt out of catalogs and solicitations from a wide range of companies. Online browser add-ons such as Ghostery, Privacy Badger, and Disconnect.me can accomplish what voluntary Do Not Track efforts have failed to do by blocking third party advertising networks from tracking consumers across different websites and apps. They do this through relatively blunt means—by blocking third-party ads entirely.[107] In the past, some consumers might have felt guilty for blocking ads on websites that are dependent upon advertising revenue for operations. However, given the failure of the ad industry to self-regulate (through Do Not Track efforts or otherwise) and the lack of other plausible alternatives to control cross-site and app tracking, consumers may find privacy-preserving ad blockers more morally justifiable. The evidence bears this out; tracker blocking add-ons have become the most popular browser extensions in recent years,[108] and

---

[103] Young people especially are migrating to more privacy-protective social media platforms. *See generally* Mary Madden et al., *Teens, Social Media, and Privacy*, PEW RESEARCH CTR. (May 21, 2013), http://perma.cc/KXB6-L4HL.

[104] Bill Budington, *Web Encryption Gets Stronger and More Widespread: 2014 in Review*, EFF (Dec. 24, 2014), https://perma.cc/Q9T7-HM2F.

[105] NATE CARDOZO ET AL., ELECTRONIC FRONTIER FOUNDATION, WHO HAS YOUR BACK? (2014), https://perma.cc/U2M4-97A4.

[106] ELECTRONIC FRONTIER FOUNDATION, SECURE MESSAGING SCORECARD (2015), https://perma.cc/S3R2-J7ZE.

[107] *See, e.g.*, *How It Works*, GHOSTERY, https://perma.cc/GS6J-ER3K.

[108] *Add-ons*, MOZILLA, https://perma.cc/Y5HR-HG7W (ranking Adblock Plus as by far the most downloaded extension; NoScript and Ghostery both in top 10); *Most Popular Google Chrome Extensions*, BEST PLUGINS, http://perma.cc/Y3AN-5RZQ (listing Adblock Plus as most popular extension).

Google Trends indicates that searches for "ad blocker" have skyrocketed since 2011.[109]

Certainly, the market for privacy is far from mature, and for most services, it is still quite difficult for consumers to effectively control the collection and distribution of their personal information. Nevertheless, the market for privacy does seem to be evolving, even as legal protections atrophy. In order for privacy controls to improve over time, consumers will need to keep demanding information control as a condition of the products they use. Self-help is not a perfect solution, and ultimately better laws need to be passed to give consumers enforceable legal rights over their data. But for the foreseeable future, it will be incumbent upon consumers themselves to take affirmative measures to protect their own privacy. Fortunately, given widespread recognition of the value of privacy, there are more and more tools available to allow consumers to take control of their information.

[109] Search for "Ad blocker," GOOGLE TRENDS, http://perma.cc/S6BD-QCP9.