Before the

Department of Commerce
National Telecommunications and Information Administration

Developing the Administration's Approach to Consumer Privacy

Docket No. 180821780-8780-01

Comments of Electronic Frontier Foundation
November 9, 2018

Submitted by:
India McKinney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
Telephone: (415) 436-9333 ext. 175
india@eff.org

For many years, EFF has urged technology companies and legislators to do a better job of protecting the privacy of technology users and other members of the public. We hoped the companies, who have spent the last decade collecting new and increasingly detailed points of information from their customers, would realize the importance of implementing meaningful privacy protections. But this year's Cambridge Analytica scandal, following on the heels of many others, was the last straw. Corporations are willfully failing to respect the privacy of technology users, and we need new approaches to give them real incentives to do better—and that includes updating our privacy laws.

EFF welcomes the opportunity to work with the Department of Commerce in crafting the federal government's position on consumer privacy. The Request for Comment published in the Federal Register identifies seven main areas of discussion: Transparency, Control, Reasonable Minimization, Security, Access and Correction, Risk Management, and Accountability. These discussion points have been thoroughly analyzed by academics over the past decades, leading to recommendations like the Fair Information Practice

Principles ("FIPPS")[1] and the previous Administration's retooling of those principles in the FTC's Consumer Privacy Framework.[2]

Thus, instead of framing our comments around these seven points, EFF will emphasize five concrete recommendations for any Administration policy proposal or proposed legislation regarding the data privacy rights of users online:

1) Requiring opt-in consent to online data gathering

2) Giving users a "right to know" about data gathering and sharing

3) Giving users a right to data portability

4) Imposing requirements on companies for when customer data is breached[3]

5) Requiring businesses that collect personal data directly from consumers to serve as "information fiduciaries," similar to the duty of care required of certified personal accountants.

Of greatest importance, any new federal data privacy regulation or statute must not preempt stronger state data privacy rules. For example, on June 28, California enacted the Consumer Privacy Act (S.B. 375) ("CCPA").[4] This is the most comprehensive state-based data privacy law, and highlights how state legislators are often in the best position to understand the needs of their constituents.[5] The law does not go into effect until 2020.

---

[1] Pam Dixon, *A Brief Introduction to Fair Information Practices*, World Privacy Forum (June 5, 2006), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[2] Federal Trade Administration, *Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report (Mar. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[3] These first four recommendations are detailed in an EFF blog. Adam Schwartz, et. al., *New Rules to Protect Data Privacy: Where to Focus, What to Avoid*, EFF Deeplinks Blog (July 2, 2018), https://www.eff.org/deeplinks/2018/07/new-rules-protect-data-privacy-where-focus-what-avoid.

[4] S.B. 375 is available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[5] EFF has and will continue to update the public about this law on our Deeplinks Blog. Adam Schwartz et. al., *How to Improve the California Consumer Privacy Act of 2018*, EFF Deeplinks Blog (Aug. 8, 2018), https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018; Adam Schwartz and Lee Tien, *EFF and Privacy Coalition Oppose Efforts to Undo California's New Privacy Law*, EFF Deeplinks

EFF is actively engaged with other privacy advocates to strengthen this law. Other states are enacting their own data privacy laws.[6] While baseline federal privacy legislation would benefit consumers across the country, any federal privacy regulation or legislation that preempts and supplants state action would actually hurt consumers and prevent states from protecting the needs of their constituents.

To be clear, any new regulations must be judicious and narrowly tailored, avoiding tech mandates and expensive burdens that would undermine competition—already a problem in some tech spaces. To accomplish that, policymakers must start by consulting with technologists as well as lawyers. Also, one size does not fit all: smaller entities should be exempted from some data privacy rules.

I. Opt-in Consent to Online Data Gathering and Sharing

Technology users interact with many online services. The operators of those services often gather data about what the users are doing on their websites. Some operators also gather data about what the users are doing on other websites by means of tracking tools. They may then monetize all of this personal data in various ways, including but not limited to targeted advertising and selling the bundled data—largely unbeknownst to the users that provided it.

New legislation could require the operator of an online service to obtain opt-in consent to collect, use, or share personal data, particularly where that collection, use, or transfer is not necessary to provide the service. The request for opt-in consent should be easy to understand and clearly advise the user what data the operator seeks to gather, how the operator will use it, how long the operator will keep it, and with whom the operator will share it. The request should be renewed any time the operator wishes to use or share data in a new way, or gather a new kind of data. And the user should be able to withdraw consent, including for particular purposes.

Some limits are in order. For example, opt-in consent might not be required for a service to take steps that the user has requested, like collecting a user's mailing address in order to ship them the package they ordered. But the service should always give the user clear notice of the data collection and use, especially when the proposed use is not part of the transaction, like renting the shipping address for junk mail.

Blog (Aug. 20, 2018), https://www.eff.org/deeplinks/2018/08/eff-privacy-coalition-oppose-efforts-undo-new-california-data-privacy-law.

[6] For example, Vermont this year passed its own data privacy law. Adam Schwartz, *Vermont's New Data Privacy Law*, EFF Deeplinks Blog (Sept. 27, 2018), https://www.eff.org/deeplinks/2018/09/vermonts-new-data-privacy-law.

There is, however, a risk that some opt-out requirements can lead to "consent fatigue." Any new regulations should encourage entities seeking consent to explore new ways of obtaining meaningful consent to avoid that fatigue. At the same time, research suggests companies are becoming skilled at manipulating consent,[7] steering users to share personal data.[8] Also, regulators should be mindful of situations where consent is coerced or buried in fine print.[9]

At present, the federal government lacks adequate authority to propose across-the-board regulation requiring Internet platforms to receive consent before the collection or disclosure of consumer data.[10] NTIA has in the past attempted to bridge this gap by convening voluntary multi-stakeholder processes. But without the force of regulation, these conversations often break down and lead to ineffective policy – like the facial recognition multi-stakeholder process that disintegrated over consent to collection, which companies were not willing to discuss.[11]

II. Right to Know About Data Gathering and Sharing

Users should have an affirmative "right to know" what personal data companies have gathered about them, where they got it, and with whom these companies have shared it (including the government).

Some limits are in order to ensure that the right to know doesn't impinge on other important rights and privileges. For example, there needs to be an exception for news gathering, which is protected by the First Amendment, when undertaken by professional reporters and lay members of the public alike. Thus, if a newspaper tracked visitors to its

---

[7] *New Analysis Shows How Facebook and Google Push Users into Sharing Personal Data*, Forbruker (June 27, 2018), https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/.

[8] Allen St. John, *CR researcher Find Facebook Privacy Settings Maximize Data Collection*, Consumer Reports (June 27, 2018), https://www.consumerreports.org/privacy/cr-researchers-find-facebook-privacy-settings-maximize-data-collection/.

[9] Dimitri Sirota, *Beyond the Privacy Fine Print: Making Privacy More Transparent*, Entrepreneur (May 10, 2017), https://www.entrepreneur.com/article/294068.

[10] In 2012, the FTC supported baseline federal privacy legislation that would grant it rulemaking authority for "notice, consent, and the transfer of information to third parties," but these bills did not move forward. *See*, *supra*, note 2 at p. 5.

[11] Jennifer Lynch, *EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-stakeholder Process*, EFF Deeplinks Blog (June 6, 2015), https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi.

online edition, the visitors' right-to-know could cover that information, but not extend to a reporter's investigative file.

California's recent privacy law creates a right to know, empowering "consumers" to obtain the following information from "businesses":

- The categories of personal information collected. *See* Sections 100(a), 110(a)(1), 110(c)(1), 115(a)(1).
- The categories of sources of the personal information. *See* Sections 110(a)(2), 110(c)(2).
- The purposes for collecting the personal information. *See* Sections 110(a)(3), 110(c)(3).
- The categories of third parties with whom businesses shares personal information. *See* Sections 110(a)(4).
- The categories of personal information sold. *See* Sections 115(a)(2), 115(c)(1).

The Act's right-to-know would be more effective if it was more granular, requiring disclosure of the specific data collected, and the data's specific sources and destinations. But it is a useful basis for conversation around this topic. And it should not be preempted by federal data privacy rules that do not provide as much transparency.

III. Data Portability

In general, users should have a legal right to export a copy of the data they have provided to an online service, in a way that provides usability for other services or functions.[12] People might use this copy in myriad ways, such as self-publishing their earlier comments on social media. Also, this copy might help users to better understand their relationship with the service provider.

In some cases, it may be possible for users to take this copy of their extracted data to a rival service.[13] For example, if a user is dissatisfied with their photo storage service, they could extract a copy of their photos (and associated data) and take it to another photo storage system. In such cases, data portability may promote competition, and hopefully over time will improve services.

---

[12] Gennie Gebhart, et. al., *What we Mean When we Say Data Portability*, EFF Deeplinks Blog (Sept. 13, 2018), https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability.

[13] Bennett Cyphers and Danny O'Brien, *Facing Facebook: Data Portability and Interoperability are Anti-Monopoly Medicine*, EFF Deeplinks Blog (July 24, 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine.

There are some situations where this right to data portability may need limits for certain services, such as social media, where various users' data is entangled. For example, suppose Alice posts a photo of herself on social media, under a privacy setting that allows only certain people to see the photo, and Bob (one of those people) posts a comment on the photo. If Bob seeks to port a copy of the data he provided to that social media, he should get his comment, but might not necessarily also get Alice's photo.

IV. Data Breach

Many kinds of organizations gather sensitive information about large numbers of people, yet fail to securely store it. As a result, such data is often leaked, misused, or stolen. What is worse, some organizations fail to notify and assist the injured parties. Victims of data breaches often suffer financial and non-financial harms for years to come.

There are many potential fixes, some easier than others. An easy one: it should be simple and fast to get a credit freeze from a credit reporting agency, which will help prevent any credit fraud following a data breach.

Also, where a company fails to adopt basic security practices, it should be easier for people harmed by data breaches—including those suffering non-financial harms—to take those companies to court.

V. Information Fiduciaries

The law of "fiduciaries" is hundreds of years old. It arises from economic relationships based on asymmetrical power, such as when ordinary people entrust their personal information to skilled professionals (doctors, lawyers, and accountants particularly). In exchange for this trust, such professionals owe their customers a duty of loyalty, meaning they cannot use their customers' information against their customers' interests. They also owe a duty of care, meaning they must act competently and diligently to avoid harm to their customers. These duties are enforced by government licensing boards, and by customer lawsuits against fiduciaries who do wrong.

Accordingly, several law professors have proposed adapting these venerable fiduciary rules to apply to online companies that collect personal data from their customers.[14] New laws would define such companies as "information fiduciaries."[15]

The effectiveness of information fiduciaries depends on the details of any proposed legislation, but they provide a tool to require companies with direct contractual relationship with their customers to use, store, and disclose customer information and collected data with due care—meaning that the company is responsible for reasonably securing the customer's data, cannot use data for a purpose other than what the data was collected for in the first place, and cannot manipulate the customer or their data solely for the company's or a third party's financial benefit.[16]

VI. Additional considerations for any data privacy rules

In addition to the basic data privacy protections discussed above, EFF hopes the NTIA will utilize the following enforcement mechanisms and rule-making norms.

- **One Size Does Not Fit All:** NTIA must take care that any of the above requirements don't create an unfair burden for smaller companies, nonprofits, open source projects, and the like. To avoid that, it should consider tailoring new obligations based on size and purpose of the service in question. For example, NTIA might take account of the entity's revenue, the number of people employed by the entity, or the number of people whose data the entity collects, among other factors.
- **Private Causes of Action**: NTIA should include one of the most powerful enforcement tools: Giving ordinary people the ability to take violators to court.

---

[14] *See* Jack M. Balkin and Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, The Atlantic (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, UC Davis Law Review (Vol 49, Apr. 2016), *available at* lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

[15] Adam Schwartz and Cindy Cohn, *"Information Fiduciaries" Must Protect Your Data Privacy*, EFF Deeplinks Blog (Oct. 25, 2018), https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy

[16] Information fiduciaries could prevent the manipulation of customers in a number of ways. For instance, the duties of care and loyalty could prevent a map app from steering hungry users to restaurants that the map app is in business with. It could also prevent a social media company from targeting users with similar political views to the company, at the detriment of users with diverging political viewpoints, and displaying ads and information about voting to only them.

- **Independent Audits**: NTIA should consider requiring periodic independent privacy audits. However, audits are not a panacea, and policymakers should attend to weaknesses in some audit processes.[17]
- **Data Collection Is Complicated:** NTIA should consult with data experts so it understands what data can be collected and used, under what circumstances.
- **Preemption Should Not Be Used To Undermine Better State Protections**: NTIA should take care not to allow weak national standards to thwart stronger state-level regulations.
- **Waivers**: Too often, users gain new rights only to effectively lose them when they "agree" to terms of service and end user license agreements that they haven't read and aren't expected to read. NTIA should consider whether and how the rights and obligations it creates can be waived, especially where users and companies have unequal bargaining power, and the "waiver" takes the form of a unilateral form contract rather than a fully negotiated agreement. We should be especially wary of mandatory arbitration requirements given that mandatory arbitration is often less protective of users than a judicial process would be.
- **No New Criminal Bans**: Data privacy laws should not expand the scope or penalties of computer crime laws. Existing computer crime laws are already far too broad.[18]

EFF welcomes the opportunity to discuss with the Department of Commerce these or any other topics regarding federal data privacy policy, federal privacy legislation, or state privacy legislation.

Respectfully submitted,

India McKinney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
Telephone: (415) 436-9333 ext. 175
india@eff.org

[17] Megan Gray, *Understanding and Improving Privacy "Audits" under FTC Orders*, Stanford (April 2018), *available at* https://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf.
[18] *Computer Fraud and Abuse Act Reform*, EFF, https://www.eff.org/issues/cfaa.