Public Knowledge

October 10, 2018

The Honorable John Thune
Chairman
Senate Committee on Commerce, Science, and Transportation
511 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Bill Nelson
Ranking Member
Senate Committee on Commerce, Science, and Transportation
716 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Thune and Ranking Member Nelson:

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we submit this statement for the record for the Senate Committee on Commerce, Science, and Transportation hearing on "Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act."

It is no longer possible to participate in society without providing data to third parties that may, in and of themselves be personal, or that, when combined with other data and analyzed, may reveal intimate information. The consequences of this data acquisition, analysis, use, and sharing can be profound for individuals' lives. For example, data have been used to show certain job postings only to men[1] and to exclude African-Americans from seeing certain housing advertisements.[2] In the 2016 election, Russian agents were able to use data to target advertisements to African-Americans to urge them not to vote.[3] Data exploitation enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination."[4] Against this backdrop, the Committee's consideration of appropriate safeguards for consumer data privacy could not be timelier.

We are pleased that the Committee appears to be taking seriously the privacy concerns facing consumers in the digital age and welcome the opportunity to submit the following principles that must be reflected in any comprehensive privacy legislation.

Scope

It is widely agreed that any comprehensive privacy legislation must cover both ISPs and edge providers.[5] However, comprehensive legislation must recognize the disparate ways that different entities use, collect, and, indeed, require personal data, and it must treat different

[1] *See* UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).
[2] Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017.
[3] Natasha Singer, *Just Don't Call It Privacy*, NY TIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.
[4] *Id*.
[5] *E.g.* INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018); U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

entities differently. For example, an ISP requires an individual's physical address in order to deliver internet service; Facebook or Twitter does not need an individual's physical address in order for their service to function. Similarly, by virtue of owning the pipes, ISPs are able to collect significantly more data about individuals than edge providers can; ISPs can view the entirety of an individual's internet activity; they also have information about whether the individual pays his or her cable bill on time. An edge provider – even one that makes prolific use of tracking pixels on third party websites – has only a fraction of an ISP's insights on a given consumer. This means that if legislation allows for exceptions for data used for legitimate business purposes,[6] it is appropriate to tailor what data are exempted for different entities (rather than, say, exempting all address information, because ISPs need it). All entities in the ecosystem should, of course, have the same obligations to protect and adhere to notice and consent requirements[7] for the data they do collect.

Additionally, the Federal Communications Commission (FCC) is the expert agency with oversight over ISPs and all communications networks; whereas, the Federal Trade Commission (FTC) is the expert agency with oversight over edge providers. There is no reason to disrupt this division of labor. Rather, comprehensive privacy legislation should build on the respective agencies' years of experience with and knowledge of the entities they oversee.

Any comprehensive privacy legislation must also reflect the ways in which data are actually used. Many edge providers do not sell data.[8] Rather, they leverage data to sell advertisements. An advertiser approaches an edge provider with an audience it would like to reach (say, suburban women with children, between the ages of 30 and 45, who like the color blue), and the edge provider uses the data it maintains to match the ad to the desired audience.[9] The fact that the data do not change hands is immaterial for consumers' experiences. Consumers are aware that companies profit off of their personal information even if that information is not sold *qua* sold. Moreover, this sort of ad targeting enables the types of nefarious advertising practices described above where women and older workers are not shown particular job postings and racial minorities are denied access to housing ads.[10]

Even where data are not sold, data may change hands in other ways. For example, researchers and app developers frequently have access to consumer data held by edge providers. At the end of March, we learned that one such app developer, Aleksandr Kogan, funneled personal information about at least 87 million Facebook users to Cambridge Analytica, a firm that purported to engage in "psychographics" to influence voters on behalf of the Trump campaign. Gallingly, as was Facebook's practice for all apps at that time, when users connected Kogan's app to their Facebook accounts, the app scooped up not only the users' personal

---

[6] For further discussion, *see* p. 5 *infra*.

[7] *See* pp. 3 – 5 *infra.*

[8] *E.g.* Kurt Wagner, *This is how Facebook uses your data for ad targeting*, RECODE, Apr. 11, 2018, https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg.

[9] *Id*. Some edge providers are also set up to find look-alike audiences with similar traits a pre-populated list an advertiser provides. Some also permit an advertiser to target particular individuals. UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

[10] *See supra* notes 1 – 3.

information, but also their friends' information – without any notice to the friends or opportunity for the friends to consent.

And, of course, data breaches continue to proliferate. Just between the time the Facebook/Cambridge Analytica news broke in March 2018 and this Committee's hearing with Mark Zuckerberg in April 2018, consumers learned of data breaches at Orbitz, Under Armour, Lord and Taylor, Saks Fifth Avenue, Saks Off Fifth, Panera Bread, Sears Holding Corp., and Delta Airlines. IBM reports that the average cost of a data breach reached $3.86 million in 2017.[11]

Given the myriad ways that personal data are collected, used, and shared, any comprehensive privacy legislation must cover the full lifecycle of consumer data, including collection, use, retention, sharing, and selling of consumer data.[12]

Sensitive/Non-Sensitive Distinction

The sensitive/non-sensitive distinction, which provides heightened protections to so-called sensitive information, like first and last name, social security numbers, bank account numbers, etc., and lesser protections to other information is increasingly illogical in today's world and should be eschewed in any comprehensive privacy legislation. Not only can so-called non-sensitive information be aggregated to reveal sensitive information, but if Facebook/Cambridge Analytica taught us anything, it is that "non-sensitive" information, like social media "likes," is useful for marketing and advertising, and also, if Cambridge Analytica (and, for that matter, the Obama campaign)[13] is to be believed, for highly sensitive activities like influencing individuals in the voting booth.

Notice and Consent

Until the digital age, individual ownership and control of one's own personal information was the basis for privacy law in the United States.[14] We should return to this principle. While we cannot avoid sharing information with some third parties, we can have greater control over that information. At a minimum, consumers should have a right to know a) what information is being collected and retained about them; b) how long that information is being retained; c) for what purposes that information is being retained; d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; e) whether and how that information is being used; f) with whom that information is being shared; g) for what purposes that information is being shared; h) under what rubric that information is being shared (for free, in exchange for compensation,

[11] IBM, COST OF A DATA BREACH STUDY (2018).

[12] In fact, even the Internet Association shares this view, writing in their own privacy principles that, "Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared . . . ". INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018).

[13] Sasha Issenberg, *How Obama's Team Used Big Data to Rally Voters*, MIT TECH. REV., Dec. 19, 2012, https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/.

[14] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry-recognized best security practices.[15]

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[16] Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. While courts have found these agreements to be binding contract, there is no reason that Congress cannot undo this presumption and insist that notice be provided in a way that consumers can quickly read and understand.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, use, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising – or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so desire.[17] In addition, service should not be contingent on the sharing of data that is not necessary to render the service.[18]

The General Data Protection Regulation (GDPR), which went into effect in Europe in May, requires some kinds of granular notice and consent, so companies already have had to figure out how to offer their users opportunities for meaningful consent. There is no reason for them not to offer the same opportunities for meaningful notice and consent in the United States. Moreover, Europe will prove an interesting testing ground, and the United States can learn from the notice and consent practices that are most effective in Europe.

---

[15] Consumer advocates are not alone in calling for meaningful notice. Both the Internet Association and The Software Alliance also call for notice. INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018) ("Transparency. Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared."); THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018) ("Transparency[.] Organizations should provide clear and accessible explanations of their practices for handling personal data, including the categories of personal data they collect, the type of third parties with whom they share data, and the description of processes the organization maintains to review, request changes to, request a copy of, or delete personal data.")

[16] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[17] This is another recommendation where advocates and industry align. *See* THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018).

[18] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, NBC NEWS, Apr. 5, 2018, https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151, such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

While it may be appropriate to allow implied consent for data that are integral to render the requested service (such as a mailing address and credit card number if one wishes to order a product on Amazon),[19] these exceptions must be narrowly drawn. Allowing companies to collect, retain, use, and share, all personal data they deem "necessary for the basic operation of the business,"[20] as the Internet Association suggests, may permit any advertising-supported platform to collect, retain, use, and share any and all consumer data. After all, if the basic operation of the business is to deliver advertising, increased data makes ad delivery more precise and efficient. Congress must ensure that any exceptions are appropriately narrowly tailored to avoid such an absurd result that would eclipse the rule.

Security

Organizations that are stewards of our personal information should be expected to adhere to recognized best practices to secure the information. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society.

Relatedly, organizations should be required to adhere to privacy by design and by default[21] and to practice data minimization.[22] The presumption should be that only data necessary for the requested transaction will be retained, absent explicit consumer consent. Organizations should be encouraged to employ encryption, pseudo-anonymization, and anonymization to protect consumers' private information, and security mechanisms should be regularly evaluated. Importantly, these evaluations must be publicly reported to enable transparency and accountability. In addition, the government should act as convener of any multi-stakeholder process to develop privacy and/or security standards. Facebook/Cambridge Analytica, as well as the cascade of recent data breaches, has demonstrated that industry cannot be trusted to police itself.

Furthermore, entities that experience a data breach should be required to notify consumers of the breach shortly after it occurs without any required showing of "harm." Since the days of Justice Brandeis, individual ownership and control of one's own personal information has been the basis for privacy law in the United States.[23] There is increasing consensus that this principle should endure in the digital age.[24] With this principle in mind, the harm occurs when

---

[19] The alternative approach, which GDPR takes, would be to allow companies to refuse service when a consumer neglects to consent to the collection and use of information required to render the requested service.

[20] INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018).

[21] Again here there are synergies with industry recommendations. *See id.*; U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

[22] *See The Code of Fair Information Practice Principles*, 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 viii (1973).

[23] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

[24] *E.g. Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary & the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. (2018) (Statement of Mark Zuckerberg, CEO, Facebook); *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy &*

personal information is acquired or accessed in a way that is unanticipated or unauthorized by the individual to whom the information pertains. As a result, individuals should be notified of a data breach upon discovery of the breach. This will allow individuals to take prophylactic measures to protect themselves from further injury.

Furthermore, the tangible harms one may be exposed to when her data are breached or shared in an unauthorized way extend far beyond the boundaries of legally-cognizable harm. For example, a data breach may expose information that could be embarrassing or that could re-endanger a domestic violence victim. Tangible harms may also come in the form of Cambridge Analytica-style "psychographics." And, the tangible injuries individuals may experience after a data breach may change as technology changes. It is impossible to foresee and legislate for all possible harms.

Moreover, codifying the harm standard simply allows the entity that has already failed to sufficiently protect sensitive personal information to determine, in its sole discretion – when it has every financial incentive to keep a data breach secret – whether or not consumers have been or will be harmed and thus whether or not consumers should be informed of the breach.

The occurrence standard is entirely workable. In fact, the GDPR adopts an occurrence standard for breach notification. Companies that notify their European customers of a breach when it occurs but that fail to notify their U.S. customers until there is demonstrable harm from the breach are likely to face backlash from their U.S. customers.

Meaningful Recourse

When there is unauthorized access to personal information, individuals must be made whole to the greatest extent possible. There are two major barriers to this. The first is the Federal Arbitration Act, which requires courts to honor the forced arbitration clauses in contracts, including forced arbitration clauses buried in the fine print of terms of service agreements. Forced arbitration clauses require consumers to settle any dispute they have with a company by arbitration rather than having their day in court – and often consumers do not even know an arbitration clause is in their contract until they go to sue. This presents three problems: 1) Arbitrators are often more sympathetic to large companies, who are repeat players in the arbitration system, than most juries would be. 2) Arbitration creates no legal precedent. 3) Frequently, it is not cost-effective for an individual to bring a claim against a large company by herself. The damages she could win likely would not exceed her legal costs. But, when customers can band together in a class action lawsuit, it becomes much more feasible to bring a case against a large company engaged in bad behavior. Forced arbitration clauses preclude class action. Congress should explicitly exempt cases addressing the failure to protect personal information from the Federal Arbitration Act to make sure consumers can have their day in court when their information is misused and their trust abused.

The second major barrier to meaningful recourse is the difficulty calculating the damages associated with unauthorized access to personal information. While one may be able to quantify

---

Commerce, 115th Cong. (2018) (Statement of Mark Zuckerberg, CEO, Facebook); Scott McDonald, President & CEO, ARF, Townhall at ARF Townhall on Research Ethics Partnered with GreenBook (Apr. 26, 2018).

her damages when her credit card information is breached or her identity is stolen, it is much harder to do so in a situation like Facebook/Cambridge Analytica. It is difficult to put a dollar amount on having one's privacy preferences ignored or her personal information revealed to third parties without her knowledge or consent. We instinctively know that there is harm in having one's personal data used for "psychographics" to influence her behavior in the voting booth, but that harm is difficult to quantify. Congress already uses liquidated damages in other situations when the damage is real, but hard to quantify. In fact, liquidated damages are already used to address other privacy harms. For example, the Cable Privacy Act provides for liquidated damages when cable companies impermissibly share or retain personally identifiable information.[25]

While the FTC can step in when companies engage in unfair and deceptive practices, the FTC is likely to only intervene in the most egregious cases. Moreover, the FTC can only extract damages from companies once they have violated users' privacy once, entered into a consent decree with the Agency, and then violated the consent decree. That means a lot of consumers must have their personal information abused before a company is held to account. Moreover, when the FTC is involved, any damages go to the government, not to making individuals whole.

We are not recommending that the FTC be taken out of the business of protecting consumers in the digital age – in fact, as described below, we believe that any comprehensive privacy legislation must strengthen the FTC (or another enforcement agency) and provide it with rulemaking authority. We are merely suggesting that consumers should also have the opportunity to protect themselves. Allowing private, class action lawsuits for liquidated damages when companies fail to safeguard private information will create the necessary incentives for companies to take appropriate precautions to protect the information they have been entrusted with. Companies, after all, understand the technology and the risks and are in the best position to develop safeguards to protect consumers.

Strong Oversight Agency with Rulemaking Authority

Any comprehensive privacy law must also be enforced by a strong oversight agency with sufficient resources and rulemaking authority. Former FTC Commissioners and staff have lamented that the FTC is not sufficiently resourced to protect consumer privacy in the digital age.[26] Since 2010, FTC funding has fallen five percent.[27] The Commission is unable pay the competitive salaries necessary to lure technologists from the private sector and as a result suffers from a dearth of technical expertise.[28] If the FTC is to be a sufficient cop on the beat protecting

[25] 47 U.S.C. § 551(f)(2)(A) (2001).

[26] *E.g.* Terrell McSweeny, Former FTC Commissioner, Open Tech. Inst., Facebook After Cambridge Analytica: What Should We Do Now? (Apr. 5, 2018); Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?*, WASH. POST, May 4, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/.

[27] David McCabe, *Mergers are spiking, but antitrust cop funding isn't*, AXIOS, May 7, 2018, https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html.

[28] Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?*, WASH. POST, May 4, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/; *see also* Terrell McSweeny, Former FTC Commissioner, Open Tech. Inst., Facebook After Cambridge Analytica: What Should We Do Now? (Apr. 5, 2018).

consumer privacy, it simply must have the resources and technical expertise commensurate with the task.[29]

Furthermore, the FTC, at present, only has the authority to respond to a privacy violation after it has occurred – in fact, the FTC is only able to impose penalties after a privacy violation has happened, the errant company has entered into a consent decree with the FTC and violated the consent decree, and the FTC has gone to court to sue the errant company. This rubric is insufficient to protect consumer privacy in the digital age. Rather, the FTC must have the ability to prevent privacy violations before they occur. The Commission needs rulemaking authority to create *ex ante* rules of the road that provide predictability for companies and sufficient privacy protections for consumers.[30]

Rulemaking authority is particularly important because of the pace at which Congress legislates. The legislative process is, in fact, designed to be slow.[31] The Telecommunications Act was last updated in 1996.[32] The Electronic Communications Privacy Act was authored in 1986 – before the advent of the World Wide Web – and has not meaningfully been updated since.[33] Google is currently rolling out an update to Gmail.[34] Apple released its latest operating system for its iPhones and iPads on September 17, 2018.[35] Congress cannot hope to keep pace with the rate at which the technology industry innovates. Therefore, it is incumbent upon Congress to empower an oversight agency, which can move more nimbly than Congress can, with rulemaking authority so that the agency can update the rules to keep up with technological changes, as well as with new harms that may arise as technology develops.

Existing Laws

We encourage Congress to enact legislation that is compatible with existing federal sector-specific privacy laws in communications, health care, finance, and other sectors, as well as with state and local privacy laws.

Moreover, while the federal government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and are much-needed cops on the beat. Even if Congress were to dramatically expand the resources available to federal privacy agencies, the federal government could not hope to provide adequate protection to consumers on its own. For example, the FTC is unlikely to get involved in a data breach

---

[29] *See* Dylan Gilbert, *The FTC Must Be Empowered to Protect Our Privacy*, PUBLIC KNOWLEDGE, June 18, 2018, https://www.publicknowledge.org/news-blog/blogs/the-ftc-must-be-empowered-to-protect-our-privacy.

[30] *See id.*

[31] Robert Pear, *The Nation; Gridlock, the Way It Used to Be*, NY TIMES, Oct. 9, 1994, https://www.nytimes.com/1994/10/09/weekinreview/the-nation-gridlock-the-way-it-used-to-be.html.

[32] *Telecommunications Act of 1996*, FCC, June 20, 2013, https://www.fcc.gov/general/telecommunications-act-1996.

[33] *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa (last visited Sept. 25, 2018).

[34] *What's new in Gmail*, GOOGLE, https://support.google.com/a/answer/7684334?hl=en (last visited Sept. 25, 2018).

[35] Matt Swinder, *iOS 12: new features and the iOS 12.1 release date*, TECHRADAR, Sept. 24, 2018, https://www.techradar.com/news/ios-12.

affecting consumers in just one state. In fact, Massachusetts Assistant Attorney General Sara Cable recently testified that less than one percent of data breaches in Massachusetts affect more than 5,000 people.[36] It is difficult to imagine federal resources being used to investigate a data breach of this size, but a state like Massachusetts might choose to get involved. In fact, Massachusetts is likely to set a breach notification standard that is more appropriate for its state than the federal government might set. For this reason, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents.

Conclusion

We appreciate the opportunity to submit this statement for the record and stand ready to assist the Committee as it continues to consider consumer privacy. If you have any questions or would like more information, please do not hesitate to reach out to me at abohm@publicknowledge.org.

Thank you,

Allison S. Bohm
Policy Counsel
Public Knowledge

CC. Members of the Senate Committee on Commerce, Science, and Transportation

[36] *Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime Before H. Comm. on Financial Services, Subcomm. on Financial Institutions and Consumer Credit*, 115th Cong. (2018) (statement of Sara Cable, Assistant Attorney General, Massachusetts).