Public Knowledge

November 9, 2018

Mr. David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Docket No. 180821780–8780–01

Dear Assistant Secretary Redl:

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 these comments in response to the National Telecommunications and Information Administration's Request for Public Comments Docket No. 180821780–8780–01: Developing the Administration's Approach to Consumer Privacy.

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, NTIA's consideration of appropriate safeguards for consumer data privacy could not be timelier.

These comments will proceed by responding in turn to the general outcomes and high-level goals for federal action NTIA has outlined, as well as by addressing some of the specific questions NTIA has posed about both the outcomes and the high-level goals. It will conclude by addressing NTIA's question about how to achieve the proposed outcomes and goals and whether any of the terms included in the request for comments requires more precise definitions. But, first, it is important to address NTIA's overarching commitment to a "risk-based approach."

---

[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*.

Risk-Based Approach: Important Considerations

Throughout the request for comments, NTIA emphasizes, "Risk-based flexibility is . . . at the heart of the approach the Administration is requesting comment on . . ."[5] Indeed, NTIA's high-level goal for federal action number four explicitly calls for "[e]mploy[ing] a risk and outcome-based approach."[6] This approach is a one-eighty from the traditional approach to privacy in the U.S. Since the days of Justice Brandeis, individual ownership[7] and control of one's own personal information has been the basis for U.S. privacy law.[8] With this principle in mind, privacy is a fundamental right, and the harm occurs when personal information is acquired, accessed, or used in a way that is unanticipated or unauthorized by the individual to whom the information pertains, regardless of the concomitant risks.

Moreover, there is substantial danger that a risk-based approach will focus solely on legally-cognizable risks, like financial loss and physical injury. These risks are a very small subset of the harms that can arise from misuse of data or data breach, and they are among the hardest harms to prove. Even where financial loss arises from a data breach or the misuse of data – say, where a credit card number is stolen and fraudulent purchases are made – it is difficult to trace that stolen credit card to one particular data breach.[9] And, where it is possible to trace back to the particular data breach, banks often reimburse customers for fraudulent purchases, obviating any actual financial loss.[10]

Furthermore, the harms one may be exposed to when her data are breached or misused extend far beyond the boundaries of legally-cognizable harm. In fact, the most pernicious harms associated with data breach and misuse of data are not currently legally-cognizable. For example, a data breach may expose information that could be embarrassing or cause reputational harm, undermining one's employment or social prospects. Data that fall into the wrong hands could re-endanger a domestic violence victim. Harms may also come in the form of Cambridge Analytica-style "psychographics," misinformation, or distortions of the public record, undermining public trust in U.S. democratic institutions. Irresponsible data use can exacerbate informational disparities, enable unfair price discrimination, limit awareness of opportunities, and contribute to employment, housing, health care, and other forms of discrimination. And, the risks associated with data use and abuse may change as technology changes.

This is not to suggest that a privacy regime must solve for all of society's ills, but it is to say that, ideally NTIA should eschew its risk-based approach for a rights-based approach. But, to the extent that the Administration's proposed privacy regime is to be based on a risk-based

---

[5] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48600 (Sept. 26, 2018); *see also id*. at 48602 (". . . should be addressed through the application of a risk and outcome-based approach.").
[6] *Id*. at 48602.
[7] When we use "ownership," we do not necessarily imply a formal, alienable property right, but rather a philosophical framework.
[8] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).
[9] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL STREET J., June 26, 2016, https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.
[10] *Id*.

approach, it must take into account the full panoply of risks – including those that may arise in the future – whether or not they are legally-cognizable under existing law.

The other pitfall of a risk-based approach is that it may tempt policymakers to further entrench the sensitive/non-sensitive distinction.[11] This 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. So-called non-sensitive information can be aggregated to reveal sensitive information, and, in fact, some non-sensitive information, in isolation, may reveal sensitive information. For example, while one's health status is frequently considered sensitive, one's shopping history is not. If one is shopping at TLC Direct[12] and Headcovers Unlimited,[13] two websites that specialize in hats for chemotherapy patients, it may be trivial to infer her health status.

Furthermore, so-called non-sensitive information can be used for purposes that are quite sensitive. For example, if Cambridge Analytica (and, for that matter, the Obama campaign)[14] is to be believed, so-called non-sensitive information like social media likes can be used for highly sensitive activities such as influencing individuals in the voting booth. In addition, sensitivity is highly subjective. Different individuals are likely to perceive different data points' sensitivity levels differently.

For these reasons, any line drawing around a sensitive/non-sensitive distinction is inherently arbitrary. Thus, any federal privacy regime must provide robust protections for all personal information – that is, any information that is reasonably linkable, directly or indirectly, to a specific consumer, household, or device[15] – and not merely for so-called sensitive information.

Privacy Outcomes

NTIA articulates a number of important privacy outcomes. This section responds to many of the proposed outcomes and, in response to question II(A)(1),[16] highlights an important additional privacy outcome.

[11] *E.g.* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018) ("[W]hich controls to offer, when to offer them, and how they are offered should . . . tak[e] into account . . . the sensitivity of the information.").

[12] TLC DIRECT, https://www.tlcdirect.org (last visited Nov. 2, 2018).

[13] HEADCOVERS UNLIMITED, https://www.headcovers.com (last visited Nov. 2, 2018).

[14] 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/.

[15] *E.g.* CAL. CIV. CODE § 1798.135(o)(1).

[16] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48603 (Sept. 26, 2018) ("Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?").

1. Transparency

Public Knowledge strongly agrees with NTIA that transparency is a "desired outcome" of any comprehensive privacy framework.[17] We have advocated that consumers 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, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry-recognized best security practices.[18]

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. We are encouraged that NTIA seems to recognize this truism, explaining that "lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding."[19] Consumers and organizations know that consumers do not typically read privacy policies or terms of service agreements. Indeed, it would be both irrational and inefficient for consumers to read privacy policies; 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.[20] Organizations 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.

NTIA has asked for guidance "as to how the privacy outcomes and goals [it articulates] can be achieved."[21] Our understanding is that the National Institutes for Standards and Technology is creating a voluntary tool to help organizations manage privacy.[22] Either in conjunction with this process or in parallel, as appropriate, NTIA should explore "nutrition label"-style approaches to privacy policies where salient information for consumers could be conveyed, in plain language, on a single cellphone screen. In general, consumer-facing privacy

---

[17] *Id*.

[18] 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.")

[19] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018).

[20] 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/.

[21] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018).

[22] Meeting with Diane Renaldo Travis Hall, Naomi Leskivitz, et. al, NTIA & NIST, in Washington, DC (Aug. 15, 2018).

policies should be concise, intelligible, clear, and prominent; they should use plain language and visualizations where appropriate.[23]

It may be appropriate for any federal privacy regime to additionally mandate a separate, legal disclosure that contains the breadth of information included in today's privacy policies and terms of service and that may, indeed, be more detailed than today's policies. The purpose of this disclosure would be a legal one – to permit the relevant administrative agency, as well as watchdog groups, to better understand organizations' data practices and hold organizations accountable when they fail to live up to their promises or when their promises fail to adhere to the law or to consumer expectations.

2. Control

As NTIA notes with its second outcome, notice alone is insufficient. Consumers must also have meaningful opportunities for "control over the collection, use, storage, and disclosure of the[ir] personal information."[24] Importantly, consumers must be able 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 or coerced as a condition of service or through manipulative design choices. As NTIA helpfully recognizes, 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.[25]

We are concerned that NTIA seems to advocate for qualified user control and seems to intend to preserve the sensitive/non-sensitive distinction within the context of user control.[26] 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),[27] these exceptions must be narrowly drawn. As described above, individual ownership[28] and control of one's own personal information has long been the basis for privacy law in the United States.[29] There is increasing consensus that this principle should endure in the digital age.[30] Permitting companies to selectively grant user control, as NTIA appears to

---

[23] *See* Information Transparency & Personal Data Control Act, H.R. 6864, 115th Cong. § 2(a)(2) (2018).

[24] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018).

[25] *Id*.

[26] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018) ("However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectation and the sensitivity of the information.").

[27] 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.

[28] When we use "ownership," we do not necessarily imply a formal, alienable property right, but rather a philosophical framework.

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

[30] *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 &*

contemplate, flies in the face of this principle. And, as described above, the sensitive/non-sensitive distinction is increasingly illogical in today's world,[31] and it is inconsistent with the principle of user control – after all, true user control would permit users to elect settings that reflect the fact that each individual defines what is and is not sensitive differently.

Furthermore, business stakeholders, such as the Internet Association, have proposed broad carve-outs from consumer control that would undermine the entire principle. For example, allowing companies to collect, retain, use, and share, all personal data they deem "necessary for the basic operation of the business"[32] 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. NTIA must ensure that any exceptions in the proposal the Administration advances are appropriately narrowly tailored to avoid such an absurd result that would eclipse the rule.

But, individual control is about more than just consent. For example, consumers should be able to port their data in a machine-readable format to another service, if they so desire.[33] And, importantly, service should not be contingent on the acquisition, use, retention, or sharing of data that is not necessary to render the service.[34]

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.

3. Reasonable Minimization

While the NTIA proposal helpfully calls for data minimization, it appears to, well, minimize its importance.[35] This is a disappointment. Data minimization is an important security measure; data that are not collected or retained are also not a target for data thieves and other malicious actors. Moreover, data minimization can help prevent some of the harms that arise from misuse of data, like unfair price discrimination, limiting awareness of opportunities, and

---

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).

[31] *See* p. 3 *supra*.

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

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

[34] 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.

[35] *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018) ("Other means of reducing the risk of privacy harm . . . can help to reduce the need for such minimization.").

perpetuating employment, housing, health care, and other forms of discrimination[36] – all risks that multiply when organizations are able to build increasingly detailed consumer profiles.

At the same time, many of the data uses that are sometimes claimed to require widespread information collection, such as machine learning, in fact do not require such copious collection, as techniques such as differential privacy[37] and federated learning[38] demonstrate. For these reasons, the presumption should be that only data necessary for the requested transaction will be retained, absent explicit consumer consent.

4. Security

NTIA is right to call on organizations to "meet or . . . exceed current consensus best practices" around security and to "secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data."[39] 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.[40] Organizations should be encouraged to employ encryption and pseudo-anonymization or de-identification to protect consumers' private information,[41] 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, organizations that experience a data breach should be required to notify consumers of the breach shortly after it occurs without any required showing of "harm." Given the philosophical consensus that individuals own their own data,[42] the harm occurs when personal information is acquired or accessed in a way that is unanticipated or unauthorized by the individual to whom the information pertains.[43] As a result, individuals should be notified of a data breach upon discovery of the breach. This will allow individuals to take prophylactic

---

[36] *See* p. 2 – 3 *supra*.

[37] *Differential Privacy Overview*, APPLE, https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (last visited Nov. 8, 2018).

[38] Brendan McMahan and Daniel Ramage, Google AI Blog, *Federated Learning: Collaborative Machine Learning without Centralized Training Data* (Apr. 6, 2017) (last visited Nov. 8, 2018).

[39] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).

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

[41] It is trivial to re-identify de-identified or pseudo-anonymized data. *See generally* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017). Therefore, any federal policy must require that organizations employ technical and policy measures to ensure that the personal data are not re-identified.

[42] When we use "ownership," we do not necessarily imply a formal, alienable property right, but rather a philosophical framework. *See* pp. 2, 5 *supra*.

[43] Additionally, traditional economic or dignitary harms may be present in fact, but difficult or impossible to demonstrate or quantify, especially for an individual.

measures to protect themselves from further injury. Moreover, entrenching the harm standard would simply allow the organization 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. Organizations 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.

5. Access and Correction

We are disappointed that NTIA only envisions giving individuals "qualified access [to] personal data they have provided" to an organization.[44] First, it is unclear in this context what "qualified" refers to. What does NTIA believe individuals should not have access to, particularly given that it is cabining the access to information the individual herself has provided to the organization?

Second, limiting consumer access to information she has provided to the organization is inappropriate. The consumer likely knows what information she has directly uploaded to the organization. While permitting her to access these data are important for data portability,[45] the more interesting and instructive information are the inferences the organization has made about her based on the information she provided.[46] It is those inferences that are most likely to facilitate some of the harms we are particularly concerned about, like unfair price discrimination, limiting awareness of opportunities, and perpetuating employment, housing, health care, and other forms of discrimination.[47] And, only by knowing about these inferences can she even attempt to guard against these harms.

By contrast, we are pleased that the ability to "rectify, complete, amend, or delete"[48] data is qualified. Individuals should not be able to "rectify" or "amend" data if the corrections they seek are inaccurate or would distort the public record. Nor should individuals be permitted to delete data where data deletion would violate others' First Amendment rights to receive information. However, individuals should have the opportunity to understand why the organizations that maintain data about them make the decisions they do and the opportunity to challenge those decisions, with a fair process, where they disagree.[49]

---

[44] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).
[45] *See* p. 6 *supra*.
[46] We recognize that there may be valid trade secrets concerns; however, a federal approach should endeavor to provide for necessary transparency without compromising trade secrets.
[47] *See* pp. 2 – 3 *supra*.
[48] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).
[49] For a much more detailed discussion, *see* JOHN BERGMAYER, EVEN UNDER KIND MASTERS: A PROPOSAL TO REQUIRE THAT DOMINANT PLATFORMS ACCORD THEIR USERS DUE PROCESS (Public Knowledge, 2018).

7. *Accountability*

We are pleased to see NTIA call for privacy-by-design,[50] for organizations to be "accountable externally and" internally for their data practices[51] and encouraged to see NTIA call for organizations "that control personal data [to] take steps to ensure that their third-party vendors and services are accountable for their use, storage, processing, and sharing of that data."[52] Such steps should include contractual provisions, as well as auditing to ensure that the contractual provisions are adhered to.

In addition, we urge the following accountability measures:

Ending Forced Arbitration: 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 an organization 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 organizations, 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 organization engaged in bad behavior. Forced arbitration clauses preclude class action. A new privacy regime 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.

Liquidated Damages: 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 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.[53]

---

[50] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018); *see* p. 7 *supra*.
[51] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).
[52] *Id*.
[53] 47 U.S.C. § 551(f)(2)(A) (2001).

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 Commission, 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,[54] we believe that any comprehensive privacy legislation must strengthen the FTC 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 organizations to take appropriate precautions to protect the information they have been entrusted with. Organizations, after all, understand the technology and the risks and are in the best position to develop safeguards to protect consumers.

Strong Agency Oversight and Enforcement: Any privacy regime must also be enforced by a strong oversight agency with sufficient resources and rulemaking authority.[55]

State Innovation and Enforcement: 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 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.[56] 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.

Additional Outcomes

In question II(A)(1), NTIA enquires about "other outcomes that should be included . . ."[57] NTIA should contemplate adding an outcome around fairness to individuals. A notice and consent regime by itself is insufficient to protect consumers in the digital age. There is an

[54] *See* pp. 13 – 16 *infra*.

[55] For a more detailed discussion of agency enforcement, see *id*.

[56] *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).

[57] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48603 (Sept. 26, 2018).

information and power asymmetry between organizations that collect data and individual consumers that makes it difficult for all but the savviest consumers to protect their personal information from misuse and abuse. Consequently, policymakers should step in to ensure that data cannot be used to unfairly discriminate against already marginalized populations. This may be achieved by perusing transparency and accountability in automated decision-making, particularly when it concerns essential services and opportunities, like housing, jobs, health care, education, and lending. If regulators, watchdog organizations, and, indeed, individuals are better able to understand algorithmic decision-making, they may be better positioned to mitigate and guard against some of the more pernicious risks associated with big data.[58]

High-Level Goals for Federal Action

NTIA articulates a number of high-level goals for federal action. This section responds to many of the proposed goals and, in response to questions II(B)(1) and II(B)(3),[59] articulates an important additional high-level goal, as well as some risks associated with NTIA's approach.

1. Harmonize the Regulatory Landscape

While we are pleased to see NTIA endorse the U.S.'s sectoral approach to privacy,[60] which defers to agencies' existing expertise and forms the backbone of U.S. privacy law, we are disappointed that NTIA appears interested in preempting state privacy laws.[61] As described above,[62] states have always served as the laboratories of democracy, legislating to address the particular needs of their residents. In addition, organizations are accustomed to innovating in an environment with "a patchwork of competing and contradictory baseline laws."[63] For example, each state has its own banking laws,[64] commercial code,[65] and environmental laws.[66] And, in Europe, GDPR is enforced by twenty-eight different member countries, each with its own implementing regulations.[67] There is no principled reason why consumer privacy should be treated differently.

---

[58] *See generally* PUBLIC INTEREST PRIVACY PRINCIPLES (2018) (included as appendix).

[59] *Id*. ("Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?").

[60] *See id.* at 48601 – 02 (Sept. 26, 2018) (NTIA "does not propose changing current sectoral federal laws." The "sectoral system provides strong, focused protections and should be maintained.").

[61] *Id*. at 48602.

[62] *See* p. 10 *supra*.

[63] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).

[64] *See* JAY B. SYKES, CONG. RESEARCH SERV., R45081, BANKING LAW: AN OVERVIEW OF FEDERAL PREEMPTION IN THE DUAL BANKING SYSTEM (2018).

[65] *Commercial Law by State*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/table_commercial (last visited Nov. 2, 2018).

[66] *Environmental Health State Bill Tracking Database*, NAT'L CONF. OF STATE LEGISLATORS (Oct. 19, 2018), http://www.ncsl.org/research/environment-and-natural-resources/environmental-health-legislation-database.aspx.

[67] *See Art. 68 GDPR European Data Protection Board*, INTERSOFT CONSULTING, https://gdpr-info.eu/art-68-gdpr/ (last visited Nov. 2, 2018).

2. *Legal Clarity While Maintaining the Flexibility to Innovate*

The best way to achieve legal clarity while maintaining the flexibility to innovate[68] is to imbue the relevant administrative agency with APA rulemaking authority. The legislative process is inherently slow and cannot hope to keep pace with technology.[69] The Telecommunications Act was last updated in 1996.[70] The Electronic Communications Privacy Act was authored in 1986 – before the advent of the World Wide Web – and has not meaningfully been updated since.[71] Google recently rolled out an update to Gmail.[72] Apple released its latest operating system for its iPhones and iPads on September 17, 2018.[73] Administrative agencies can move more nimbly than Congress, can articulate clear rules of the road, and can update those rules as technology changes in order to ensure that innovation continues without sacrificing individuals' privacy and autonomy or American values.

3. *Comprehensive Application*

NTIA advocates a consumer privacy regime that applies "to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws."[74] While it is widely agreed that any comprehensive privacy legislation must cover both ISPs and edge providers,[75] comprehensive legislation must recognize the disparate ways that different organizations use, collect, and, indeed, require personal data, and it must treat different organizations 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 browsing 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,[76] it is appropriate to tailor what data are exempted for different organizations (rather than, say, exempting all address information, because ISPs need it). All

---

[68] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).
[69] 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.
[70] *Telecommunications Act of 1996*, FCC, June 20, 2013, https://www.fcc.gov/general/telecommunications-act-1996.
[71] *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).
[72] *What's new in Gmail*, GOOGLE, https://support.google.com/a/answer/7684334?hl=en (last visited Sept. 25, 2018).
[73] Matt Swinder, *iOS 12: new features and the iOS 12.1 release date*, TECHRADAR, Sept. 24, 2018, https://www.techradar.com/news/ios-12.
[74] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).
[75] *E.g.* INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018); U.S. CHAMBER, PRIVACY PRINCIPLES (2018).
[76] For further discussion, *see* p. 5 *supra*.

organizations in the ecosystem should, of course, have the same obligations to protect and adhere to notice and consent and other requirements[77] 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 organizations they oversee.

4. Employ a Risk and Outcome-Based Approach

For a fulsome discussion of this goal, please see *supra* pp. 2 – 3.

5. Interoperability

NTIA is correct that facilitating cross-border data flow is imperative in today's interconnected, global society. It is perplexing, however, that NTIA appears solely concerned with "developing a regulatory landscape that is consistent with the international norms and frameworks in which the United States participates."[78] The request for comments specifically references the APEC Cross-Border Privacy Rules.[79] Glaringly absent from the request for comments is any reference to GDPR or Privacy Shield – even though re-negotiations of Privacy Shield are ongoing, U.S. compatibility with GDPR may be relevant for those negotiations, and countries, such as Brazil, are adopting GDPR-like models.[80] This is not to say that the United States should copy GDPR whole-cloth. Portions of GDPR would be culturally or even legally inappropriate and/or unworkable in the United States.[81] However, U.S. policymakers should consider interoperability with GDPR, as well as lessons learned from GDPR implementation, when developing the U.S. consumer privacy regime.

7. FTC Enforcement

As described above, any comprehensive privacy law must be enforced by a strong oversight agency with sufficient resources and rulemaking authority, and if a federal privacy regime vests enforcement primarily with the FTC, it must ensure that the FTC has sufficient authority and resources to undertake the mandate.

---

[77] *See* pp. 4 – 6 *supra.*

[78] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).

[79] *Id*.

[80] Melanie Ramey, *Brazil's New General Data Privacy Law Follows GDPR Provisions*, INSIDE PRIVACY, COVINGTON & BURLING LLP, Aug. 20, 2018, https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/; Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIVACY L. & BUS. INT'L REP. 10, 10 – 13 (2017).

[81] *See generally* Gus Rossi, *Is the GDPR Right for the United States?*, PUBLIC KNOWLEDGE, Apr. 9, 2018, https://www.publicknowledge.org/news-blog/blogs/is-the-gdpr-right-for-the-united-states.

Former FTC Commissioners and staff have lamented that the FTC is not sufficiently resourced to protect consumer privacy in the digital age.[82] Since 2010, FTC funding has fallen five percent.[83] 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.[84] If the FTC is to be a sufficient cop on the beat protecting consumer privacy, it simply must have the resources and technical expertise commensurate with the task.[85]

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.[86]

It is also unlikely that the FTC's unfair and deceptive acts and practices (UDAP) authority is sufficient to protect individuals' privacy in the digital age. An organization's privacy or data security practice is deceptive if, "'first, there is a representation, omission, or practice that, second, is likely to mislead consumers acting reasonably under the circumstances, and third, the representation, omission, or practice is material.'"[87] While the FTC has been able to use its deceptiveness authority to draw attention to and ameliorate some companies' privacy violative practices,[88] it is an insufficient overall solution, because deceptiveness only applies when an organization has lied or been misleading about its privacy practices.

---

[82] *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/.

[83] 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.

[84] 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).

[85] *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.

[86] *See id.*

[87] *FTC v. AMG Servs.*, 29 F. Supp. 3d 1338, 1364 (quoting F.T.C. v. Gill, 265 F.3d 944, 950 (9th Cir. 2001)).

[88] *E.g.* Lesley Fair, What Vizio was Doing Behind the TV screen, FED. TRADE COMM'N, (Feb. 6, 2017, 11:05 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what- vizio-was-doing-behind-tv-screen; Tech Company Settles FTC Charges it Unfairly Installed Apps on Android Mobile Devices Without Users' Permission, FED. TRADE COMM'N (Feb. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/tech-company-settles-ftc-charges-it-unfairly-installed-apps; HTC America Settles FTC Charges it Failed to Secure Millions of Mobile Devices Shipped to Consumers, FED. TRADE COMM'N (Feb. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile; Grant Gross, FTC Warns App Developers Against Using Audio Monitoring Software, CIO (Mar. 18, 2016), http://www.cio.in/news/ftc-warns-app-developers-against-using-audio-monitoring-software; Aaron's Rent-To-Own Chain Settles FTC Charges that it Enabled Computer Spying by Franchises,

The FTC's unfairness authority is even more complicated. Rather than enumerate particular unfair practices, Congress envisioned unfairness keeping pace with technology and "designed the term as a 'flexible concept with evolving content.'"[89] In order to qualify as "unfair," the injury the practice causes must be "[1] substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided."[90] This is a high bar in and of itself. It requires a cost-benefit analysis.[91] And, in many cases, even if the FTC is able to demonstrate a legally-cognizable harm – as described above, a challenging prospect[92] – the consumer may benefit from the practice, because, for example, pervasive data collection may reduce her search time and enable businesses to show her more relevant advertisements. Or, competition may benefit, because, for example, it may be less expensive for a new entrant to enter the market if it does not have to pay the money necessary to adhere to the latest security standards. Finally, in some cases, the consumer could have avoided the harm by declining to sign up for the particular service or buy the particular product.

In addition to the high bar set by the unfairness factors themselves, the Eleventh Circuit in *LabMD* recently concluded that an unfair act or practice must be "clear and well-established," that is, "expressed in the Constitution, statutes, or the common law."[93] The court did signal that this requirement does not dictate that the FTC spell out precisely what portion of Constitution, statute, or the common law it is relying upon. Rather, the Eleventh Circuit noted that the source of the clear and well-established principle could be "apparent"[94] Still, this would seem to confine the FTC to serving – in some cases, such as when the clearly established law is the common law of torts – as a second enforcement mechanism for existing laws, rather than allowing the concept of unfairness to evolve as Congress intended.[95, 96]

FED. TRADE COMM'N (Oct. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer; Spyware Seller Settles FTC Charges; Order Bars Marketing of Keylogger Software for Illegal Uses, FED. TRADE COMM'N (June 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/spyware-seller-settles-ftc-charges-order-bars-marketing-keylogger.

[89] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015) (quoting *FTC v. Bunte Bros*, 312 U.S. 349, 353 (1941)).

[90] *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018), at *12 (internal citations omitted).

[91] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 255 (3d Cir. 2015).

[92] *See* p. 2 *supra*.

[93] *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018), at *16.

[94] *Id.*, at *16 – 17 ("The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used . . . It is apparent to us, though, that the source is the common law of negligence.")

[95] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015) (quoting FTC v. Bunte Bros, 312 U.S. 349, 353 (1941)).

[96] *LabMD* creates something of a circuit split with the Third Circuit, which held in *FTC v. Wyndham Worldwide Corp.* that an organization subject to the FTC's unfairness authority need only have "fair notice that its conduct could fall within the meaning of the" FTC Act; it is not entitled to "to know with ascertainable certainty the FTC's interpretation of what . . . practices are required by" the act. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d at 255. The Third Circuit reasoned that Wyndham had reason to know that "cybersecurity practices can, as a general matter, form the basis of an unfair practice." *Id.* It did not peg its reasoning to the idea that unfair cybersecurity practices violate clear and well-established law. Indeed, even the Eleventh Circuit in *LabMD* acknowledged that "Congress 'intentionally left development of the term 'unfair' to the Commission' through case-by-case litigation." *LabMD,*

In sum, if a federal privacy regime is to rely on FTC enforcement, the agency must be able to enforce based on more than just its UDAP authority, and it requires commensurate resources and rulemaking authority.

Finally, we are heartened that NTIA envisions "certain exceptions made for sectoral laws outside the FTC's jurisdiction, such as HIPAA,"[97] given that sectoral privacy laws form the foundation of the U.S. privacy regime. Because the FCC is the expert agency with oversight over ISPs and all communications networks, we expect that the FCC will also be afforded an exception that allows it to enforce any privacy law with respect to ISPs and communications networks.

8. Scalability

NTIA rightly takes the viability of third parties into account in its request for comments, writing "small businesses that collect little personal information and do not maintain sensitive information about their customers should not be the primary targets of privacy-enforcement activity, so long as they make good-faith efforts to utilize privacy protections."[98] The caveats NTIA includes – collecting little personal information, not maintaining information, making good faith efforts to utilize privacy protections – are important. While a federal privacy regime should have as a goal allowing for competition and allowing new entrants to enter the market relatively easily, competition cannot come at the expensive of certain fundamental privacy protections. For example, a new entrant that is unable to sufficiently secure consumers' personal information from breach and unauthorized access probably should not be able to enter the market.

In addition, while a "distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations"[99] may be desirable, this regime must allocate responsibility between organizations that control personal data and third-party vendors. For example, a federal privacy regime should require contractual provisions, as well as auditing to ensure that the contractual provisions are adhered to, making clear that the third-party vendors will adhere to any privacy requirements the organization that controls personal data is subject to. And, a federal regime should delineate who has the obligation to inform consumers in the event of a third-party vendor's data breach.

Additional Goals

In question II(B)(1), NTIA solicits "other goals that should be included."[100] Much as we articulated above a potential goal around fairness, it would be helpful to have a high-level goal

Inc. v. FTC, No. 16-16270 (11th Cir. June 6, 2018), at *10 (internal citations omitted). Still, *LabMD* likely makes the already hard-to-satisfy standard for "unfairness" harder to satisfy.

[97] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).

[98] *Id*. at 48603.

[99] *Id*.

[100] *Id*.

around protecting individuals from unlawful discrimination based on their data and advancing equal opportunity.[101]

In addition, it would be helpful to have a high-level goal around meaningful redress for consumers in the event of privacy violations. This goal is an important corollary to NTIA's proposed accountability outcome, and we've articulated much of what that goal should look like in that section of these comments.[102]

Risks

NTIA also enquires about risks associated with its goals or overall approach.[103] Although not stated as an explicit goal, fostering innovation appears to be a goal underpinning the entire request for comments.[104] While fostering innovation is a laudable goal, and Public Knowledge strongly supports a competitive marketplace as a cornerstone of the U.S. economy,[105] the desire for innovation should not be used as a red herring to undermine important privacy protections. As described above, businesses have always innovated in an environment with disparate state laws.[106] And, as Dr. Andrea Jelinek, chair of the European Data Protection Board, testified before the Senate Commerce Committee, new entrants into the market in Europe simply take GDPR into account and employ privacy-by-design and by default into their products from the beginning; Europe has not seen a decline in innovation since GDPR implementation.[107] There is no reason to believe that privacy and innovation are a zero-sum game.

C. Next Steps

NTIA asks about "next steps and measures the Administration should take to effectuate the . . . privacy outcomes, and to achieve an end state in line with the high-level goals."[108] The majority of the proposals in these comments would require comprehensive privacy legislation to actualize, and the President should make clear his preference for, and willingness to sign, comprehensive privacy legislation.

But, there are some actions the executive branch could take in the absence of privacy legislation. For example, the FTC could consider possession of personal data as a potential barrier to entry during merger review, even when a merger would not otherwise have significant vertical or horizontal competitive effects. The FTC could also use its UDAP authority to explore,

---

[101] *See* pp. 2 – 3 *supra; see generally* PUBLIC INTEREST PRIVACY PRINCIPLES (2018) (included as appendix).

[102] *See* pp. 9 – 10 *supra.*

[103] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48603 (Sept. 26, 2018).

[104] *E.g. id*. at 48600 ("Through this Request for Comment (RFC), the Administration will determine the best path toward protecting individual's [sic] privacy while fostering innovation.").

[105] *Competition*, PUBLIC KNOWLEDGE, https://www.publicknowledge.org/issues/detail/competition-policy (last visited Nov. 5, 2018).

[106] *See* p. 11 *supra*.

[107] *Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 115th Cong. (2018) (statement of Andrea Jelinek, Chair, European Data Protection Board).

[108] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48603 (Sept. 26, 2018).

through case-by-case adjudication whether it is deceptive for organizations to place third party trackers across the internet, tracking even those individuals who do not have an account with the particular organization. The FTC could also conduct a 6(b) study of how organizations use data and how that data usage affects competition. Because a 6(b) study results in a public, published report, this study should provide useful background for advocates, policymakers, and the public in the ongoing debate over privacy in the digital age. In addition, the President should include in his annual budget request increased resources for the FTC that might enable the agency to hire the technologists and lawyers necessary to tackle its expansive mandate.[109]

D. Definitions

NTIA enquires about what terms in its request for comment require definition and asks for recommended definitions.[110] At least three terms require definition. The first is "reasonable." In many ways, this request for comments hangs its hat on reasonableness, focusing on a "reasonably informed consumer"[111] with "reasonable control over the collection, use, storage, and disclosure" of her personal information,[112] as well as on "reasonable minimization,"[113] "reasonable security measures,"[114] and reasonable ability to "access and correct" personal data.[115] However, the term reasonable is ambiguous, and companies, consumers, and advocates are unlikely to collectively agree on what the term means. We urge the adoption of a definition of "reasonableness" that focuses on consumer perception – after all, it is their personal information that hangs in the balance – and not merely on what companies find most advantageous for their bottom lines. Right now, because, as described above, many privacy harms are not legally-cognizable and those that are legally-cognizable are difficult to prove,[116] organizations are able to externalize the cost of protecting consumer privacy, forcing consumers and the public at large to bear the burdens associated with data breach and irresponsible collection, use, storage, and sharing of personal information. The definition of reasonableness should force companies to internalize these externalized costs.

"Risk" is also undefined in NTIA's request for comments. As described in detail above,[117] "risk" must be defined to include the full panoply of harms that arise from misuse of data and data breach, and not merely legally-cognizable harms.

Finally, NTIA's request for comments neglects to include a definition of "personal information." That definition should be something to the effect of personal information means any information that identifies, relates to, describes, is capable of being associated with, or could

[109] *See* pp. 13 – 16 *supra*.
[110] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48603 (Sept. 26, 2018).
[111] *Id*. at 48601.
[112] *Id*.
[113] *Id*.
[114] *Id*. at 48601 – 02.
[115] *Id*. at 48602.
[116] *See* p. 2 *supra*.
[117] *See* pp. 2 – 3 *supra*.

reasonably be linked, directly or indirectly, with a particular consumer, household, or device.[118] A broad definition that includes inferences made from personal information is exceedingly important, because consumers are less likely to be aware of the information organizations infer about them, and, moreover, inferences are likely to facilitate many of the most pernicious harms privacy legislation should guard against, like unfair price discrimination, limiting awareness of opportunities, and perpetuating employment, housing, health care, and other forms of discrimination.[119]

E. FTC Resources

NTIA asks specifically about the "changes [that would] need to be made with regard to the FTC's resources, processes, and/or statutory authority" in "order to achieve the goals laid out in" its request for comments.[120] For a fulsome response to this question, please see *supra* pp. 13 – 16.

Conclusion

We appreciate the opportunity to comment on NTIA's Request for Public Comments Docket No. 180821780–8780–01: Developing the Administration's Approach to Consumer Privacy and stand ready to assist NTIA as it continues to develop the Administration's approach to consumer privacy.

Sincerely,

Allison S. Bohm
Policy Counsel
Public Knowledge

[118] *E.g.* CAL. CIV. CODE § 1798.135(o)(1).
[119] *See* p. 2 – 3 *supra*.
[120] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48603 (Sept. 26, 2018).

Appendix

Public Interest Privacy Legislation Principles

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[121] people think they lack control over their data,[122] want government to do more to protect them,[123] and distrust social media platforms.[124]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[125] (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across

---

[121] *The State of Privacy in Post-Snowden America*, Pew (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.
[122] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, Consumer Reports (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data.
[123] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.
[124] *Id.*
[125] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.