ConsumersUnion®

THE ADVOCACY DIVISION OF CONSUMER REPORTS

November 9, 2018

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

Request for Comment on the Administration's Approach to Consumer Privacy

Dear Assistant Secretary:

Consumers Union (CU), the advocacy division of Consumer Reports,[1] is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. We write to respond to the request for comment on the Administration's approach to consumer privacy posed by the National Telecommunications and Information Administration (NTIA).

Americans have a fundamental right to privacy and therefore deserve strong privacy protections under the law. Consumers Union is committed to improving transparency and incentivizing the market to more sufficiently protect consumers' personal information through product testing and consumer empowerment under the Digital Standard.[2] However, for consumers to be fully protected companies must be required to comply with data security and privacy standards, and face real consequences for failure to do so. Consumers need stronger privacy laws *now* in order

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] The Digital Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use every day. *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

to take control of their personal data and digital security. And Americans not only need but desire greater rights and protections in a world of universal surveillance and connectivity.[3]

A federal privacy law should require: (1) reasonable data minimization tied to context and consumer expectations; (2) user permission for extraneous data collection and sharing; (3) detailed information about data practices to ensure accountability; (4) strong data security practices; (5) ways for consumers to get easy access to their information; and (6) strong enforcement to deter wrongdoing.[4] In addition, a federal privacy law should not preempt stronger state laws; a federal law should create a floor for privacy protections and not a ceiling. States have always been our "laboratories of democracy"[5] and should be permitted to create stronger laws to protect their consumers from new and emerging threats.

Below we have commented on the specific aspects of the Privacy Outcomes and High-Level Goals for Federal Action as expressed by the NTIA.

A. Privacy Outcomes

Consumers Union supports the NTIA's effort and agrees on many of the Privacy Outcomes outlined by the NTIA. However, we suggest some reordering modification to the Outcomes. We provide specific feedback on those elements below.

1. Risk Management[6]

As an initial matter, we urge the NTIA to reverse its misguided tethering of consumer protections to subjective assessments of privacy *risk* and *harm* and to eliminate the Privacy Outcome of *Risk Management*. Rather, the framework should recognize that consumers will always have a privacy *interest* in data collection, use, retention, or sharing because once private information is in the hands of another there is *always* a chance of some misuse. For example, data collected in the past could be publicly breached, accessed through mandatory legal process, or used for price

---

[3] Jessica Rich, *Beyond Facebook, It's High Time for Stronger Privacy Laws*, WIRED (Apr. 8, 2018), https://www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws/.

[4] *Where We Stand: Congress Should Pass A Strong Privacy Law*, Now, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/.

[5] U.S. Justice Louis Brandeis in NEW STATE ICE CO. V. LIEBMANN, 285 U.S. 262 (1932).

[6] "Organizations should take steps to manage the risk of disclosure or harmful uses of personal data. Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes." *Developing the Administration's Approach to Consumer Privacy, Request for Comment*, NAT'L TELECOMMC'N & INFO. ADMIN. (Sept. 26, 2018), fhttps://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy.

discrimination to decrease a consumer's share of consumer surplus from any transaction.[7] From the perspective of the consumer, there is *necessarily* privacy risk when someone else has their data. With limited exceptions, a privacy law's protections should not be contingent upon a company's own (and necessarily biased toward its own interests) evaluation of how significant those risks are.

And for this very reason, while the United States has fewer privacy protections than other countries, the laws we have passed have not been artificially constrained by *ad hoc* determinations of privacy risks or harms. The Wiretap Act,[8] for example, does not ask potential eavesdroppers to weigh the relative harms and benefits to determine the legality of intercepting a potential communication. Nor does the Video Privacy Protection Act[9] allow someone to make subjective judgments about how "harmful" the release of someone's viewing habits might be. Rather, the laws' protections apply *per se*, obviating any risk analysis, leading to clearly stronger protections and more clear and predictable rules for everyone.

Because the proliferation of data is, to the consumer, unpredictable and hard to control, the law's protections should apply *per se* protections for privacy intrusions. Potential harms to the consumer may not be obvious when the data is first collected because data collected in the past could be used in new and unexpected ways. In addition, risk assessment introduces unnecessary uncertainty into the law, both for companies and consumers (who might not necessarily agree on what constitutes an acceptable privacy risk).

Furthermore, in practice these risk assessments will be made (often opaquely) by companies with skewed incentives to allow data processing and disregard consumer interests. Even then, such assessments will not always be rational: businesses are run by humans, and humans exhibit a natural human tendency to overestimate a small chance of something good happening and to underestimate the chances of something bad happening.[10] This is a core tenet of behavioral economics, and explains why people play the lottery despite the odds and decreasing marginal value of money, or do not buckle their seat belts despite the low cost and tremendous risk. Translated to data privacy, companies will tend to undervalue data security, and undervalue data minimization as well, discounting the likelihood of a security event, but overly optimistic about the potential for found wealth in data troves. Therefore, a consumer privacy protections

---

[7] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[8] 18 U.S. § 2511.

[9] 18 U.S.C. § 2710.

[10] Klaus Mathis & Ariel David Steffen, *From Rational Choice to Behavioural Economics*, UNIV. OF LUCERNE (2015) https://www.unilu.ch/fileadmin/fakultaeten/rf/mathis/Dok/1_Mathis_Steffen_From_Rational_Choice_to_Behavioural_Economics.pdf.

framework should reflect the reality of human nature, and eliminate opportunities for skewed incentives and irrational tendencies to weaken privacy protections.

Security, on the other hand, is one area where a risk-based framework is reasonable. Security necessarily involves a balancing of costs and the potential harms from inadvertently exposed data. Companies should consider possible ill effects when they are deciding how much to spend on a potential loss. For other Privacy Outcomes, such as data minimization, access, and transparency of practices, the rules should be bright-line.

2. Data Minimization[11]

We urge NTIA to make *Data Minimization* the leading principle of its privacy framework to reflect the amount of work this one principle should shoulder. Many of the concerns currently addressed in the *Control* principle should instead be resolved by a clear and comprehensive expectation of data minimization.

Data minimization, done correctly, would redistribute the onus of good data practices onto the company and off of the consumer. Consumers are already overwhelmed with the number of decisions they are asked to make. Consumers should be empowered to use products without fear that the service or product will mine and collect more data than the consumer would reasonably expect. Ever-present pop-up dialogs and byzantine user controls do not serve users well; instead, consumers should be entitled to expect that data collection and sharing will be limited to the context of their interactions with any given company.

Specifically, a business that collects a consumer's personal information should limit its collection and sharing of personal information with third parties to *what is reasonably necessary to provide a service or conduct an activity that a consumer has requested*. Additional data collection or sharing should only happen with a user's clear and informed permission (*see infra* Section A(3): *Control)*. Such a principle could have narrow exceptions—such as allowing collection or sharing as is reasonably necessary for security or fraud prevention. Additionally, some related, operational processing of already-collected data should be allowed without bothering the user for permission—such as first-party analytics, research, and marketing.[12]

---

[11] "The collection, use, storage and sharing of personal data should be reasonably minimized in a manner proportional to the scope of privacy risks. Other means of reducing the risk of privacy harm (e.g., additional security safeguards or privacy enhancing techniques) can help to reduce the need for such minimization."
Developing the Administration's Approach, *supra* note 6.

[12] However, due to the breadth of the security/fraud exception and the potential for this exception swallowing the rule, data collected or retained solely for security or fraud prevention should not be used for related operational purposes.
This approach to consumer data dovetails with Professor Jack M. Balkin's concept of "information fiduciaries" in which the company must be loyal to the consumer's interests and show a duty of care to the data collected. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, FACULTY SCHOLARSHIP SERIES 5154 (2016), https://digitalcommons.law.yale.edu/fss_papers/5154.

We also urge the NTIA to remove the option to employ additional safeguards or privacy-enhancing techniques (other than robust de-identification) in order to reduce the need for data minimization. Data minimization is, in of itself, a principle that should be comprehensively stated here without giving companies other options that do not work to satisfy the consumer's concerns, preferences, and expectations. Additional safeguards and/or privacy controls are not sufficient substitutes for data minimization. Companies should employ safeguards as a part of their reasonable data practices and not as a shield in order to continue to scoop up excessive consumer information.

3. Control[13]

Although *Data Minimization* should be doing most of the work for these principles, if a company wants to engage in additional, non-contextual data collection or sharing, it should obtain the consumer's permission to do so. This request should be relatively rare, as most consumers are unlikely to want unrelated data collection absent a compelling value proposition. We urge industry and the NTIA to avoid a model that follows the cookie consent banners in Europe, which often confusingly conflate both contextual, first-party collection and usage with non-essential third-party sharing for advertising.

Since consumers do not expect their data to be shared by a company with a third party, such sharing should not occur without the consumer's prior affirmative consent. Therefore, under this principle the user's ability to control their personal information should extend to personal information that is obtained from third parties as well as first-party interactions. Unfortunately, the *Control* section does not currently cover third parties. Without the inclusion of third-party data on individuals, this requirement is undermined by that loophole. Finally, consumers need the ability to request deletion of their account information as one aspect of their ability to control their data.

Consumers should be entitled to the reasonable expectation that companies do not collect more or different types of data than what is reasonably necessary for a requested service. Therefore, companies should have to get the consumer's opt-in consent for additional data collection or sharing, in response to a dedicated prompt that is not tied to other boilerplate disclosures or other permissions, in order to conduct this excess data collection. A consumer's consent should be freely given. Further, as we discuss *infra* at the end of Section A, we oppose pay-for-privacy

[13] "Users should be able to exercise control over the personal information they provide to organizations. 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 expectations and the sensitivity of the information. The controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making. In addition, controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity." *Developing the Administration's Approach*, *supra* note 6.

schemes and urge the NTIA to include a prohibition against discriminatory treatment of a consumer on the basis of their exercise of these controls.

If a company wants to engage in out-of-context data collection or sharing, it should make a clear and compelling case to the consumer and only proceed with permission. An opt-out approach is inconsistent with consumer demands and expectations. If the NTIA insists on advocating for an opt-out regime, the control needs to be scalable in order for the consumers' choices to be uniformly implemented across the digital spectrum. Opt-outs should be powerful and universal. In the past, we have seen opt-outs that lack the ability to scale or the requirement that all entities respect the opt-out which fails to protect consumers. Unfortunately, as tracking technology has gotten more invasive, we have also seen the collapse of industry efforts to self-regulate. The same weaknesses that existed years ago in the online marketplace largely persist to this day: the rules only apply to coalition members; industry opt-outs are fragile and easily overridden; industry opt-outs only address usage and do not impose meaningful collection or retention limitations; and notice and privacy interfaces were seriously flawed.[14] One strong example of a powerful and universal opt-out for consumers is encapsulated in Senator Ron Wyden's discussion draft of the *Consumer Data Protection Act*,[15] which establishes a national Do Not Track system that would permit consumers to stop third-party companies from tracking them on the web by sharing data, selling data, or targeting advertisements based on their personal information. Furthermore, the bill requires the use of device-level signifiers such as "Do Not Track" instructions for unauthenticated consumer data divorced from real world identifiers.

Consumers should have policy controls that prevents companies from evading their tracking preferences. We hope the NTIA principles help foster an environment in which consumers are provided with these controls and the ability to exercise them easily.

4. Transparency[16]

Consumers lack transparency for how their data is collected, used, shared, stored, and deleted. Individual Americans need more transparency around those practices in addition to what specific information is being collected about them. While the California Consumer Privacy Act (CCPA)

---

[14] *Statement of Justin Brookman Before the U.S. Senate Comm. On Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.

[15] *Consumer Data Protection Act, Discussion Draft*, SENATOR RON WYDEN (Nov. 1, 2018), https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf.

[16] "Organizations should be transparent about how they collect, use, share, and store users' personal information. Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information. Transparency can be enabled through various means. Organizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, 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. Organizations should use approaches that move beyond this paradigm when appropriate." *Developing the Administration's Approach*, *supra* note 6.

provides California residents with the ability to find out the categories and specific pieces of personal information that has been collected about them, the federal privacy framework should require more transparency from companies. In addition, the privacy policies that companies provide should specify what data they are collecting and when.

Although lengthy disclosures at the initial point of interaction have not fostered sufficient consumer understanding, companies should still be required to provide these disclosures and be more transparent and explicit about their data collection and practices. While few consumers read privacy policies, detailed disclosures should be written for the groups that already read them: regulators, reporters, and consumer-protection organizations like Consumer Reports. All of these entities are engaged in monitoring privacy policies for policy, consumer protection, and investment purposes and should continue to do so, but with more explicit information at hand. Today's policies are often vaguely expansive, providing little reliable concrete information about companies' actual practices. A transparency mandate to provide more precise information could remedy that.

Detailed disclosures will allow for experts to assess and provide consumers with better information and tools to evaluate and compare their privacy choices. For instance, in order to provide consumers with more information about their options, Consumer Reports and its partners developed The Digital Standard,[17] an open standard for testing products for privacy and security in order to help consumers make informed decisions in the marketplace. The testing includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies. This effort depends on the transparency that privacy policies and user interfaces provide consumers. In addition, one of the important criteria under our Digital Standard is that the user can see and control everything the company knows about the individual. In order for a company's data practices to be responsible under the Standard, the company must enable the consumer to be able to know what user information the company is collecting, must only request and collect information that is needed to make the product or service work correctly, and must explicitly disclose every way in which it uses the individual's data.[18]

[17] *The Standard*, *supra* note 2.
[18] *Id*.

4. Security[19]

Companies should be required to implement reasonable security measures appropriate to the nature of the information in their control, including administrative, technical, and physical safeguards, with sufficient penalties for wrongdoing. Connected devices and the data they collect and transmit should be protected as well. This is important, because the United States has a surprisingly inadequate data security infrastructure. Less than half of the states have a general-purpose data security requirement,[20] and Federal Trade Commission (FTC) enforcement of data security under its Section 5 authority is not sufficient to protect consumers.

The current federal data security regime covering most companies—characterized by self-regulation backed up only by FTC enforcement under Section 5—under incentivizes good data security practices. While the FTC has used Section 5 of the FTC Act extensively to punish unreasonable data and cyber security practices, the FTC use of unfairness to require reasonable security has been challenged (sometimes successfully) in court. Moreover, the FTC's effectiveness is limited by certain restrictions on its authority. It has very limited rulemaking authority. And it can only seek penalties for law violations in very specific instances. An affirmative data security law would give the FTC more authority to protect consumers, not less, including: stronger tools to protect consumers from security threats so long as it included stronger remedies to hold wrongdoers accountable, and greater resources to address consumer harms across the entire marketplace.

5. Access and Correction[21]

Consumers should have the ability to access the actual data that companies have on the individual and not just categories of data. The CCPA, which will go into effect in 2020, provides Californians with important new consumer protections, including the right to request that

---

[19] "Organizations should employ security safeguards to protect the data that they collect, store, use, or share. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure. Further, organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available. Organizations should secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data." *Developing the Administration's Approach*, *supra* note 6.

[20] *Data Security Laws, Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (Oct. 15, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[21] "Users should be able to reasonably access and correct personal data they have provided. This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation." *Developing the Administration's Approach*, *supra* note 6.

companies provide consumers the categories and specific pieces of personal information collected about them.[22] Federal law should expand those protections to all Americans.

In addition, data portability is not addressed in this section. Consumers need the ability to not only see what data companies have about them but also the right to take their consumer data elsewhere. Without this element, consumers will be locked into one service or product and will be unable to exercise their preferences. This is especially important with regards to consumers' ability to trust the companies they currently interact with. For example, a consumer could desire to move their data to another company due to a recent breach or misuse of their data by the current company they use or interact with. Without data portability, consumers will be blocked or highly disincentivized from exercising this option. In addition, data portability allows for greater competition in the marketplace. If consumers are not able to take their data to a new company, the market will strongly preference entrenched legacy organizations and not foster an innovative business landscape.

Finally, a comprehensive tenet on data access and correction should include some level of authentication for the end-user who is requesting access. While authentication is undesirable for other elements in these principles, the ability to assess the identity of the requestee is necessary to ensure the security of the data that the company controls about an individual. Without such a measure, malicious actors could gain access to the personal data companies have about an individual.

6. Accountability[23]

We urge the NTIA to include significant consequences for companies when these principles are not followed under this *Accountability* section. Accountability means consequences for actions—it does not simply mean having an internal privacy program. Any effective data protection law needs to pair substantive requirements with strong enforcement in order to sufficiently protect consumers. A law that favors process mandates over substantive controls will not serve consumers, but rather simply enrich compliance lawyers.

In addition, although we support this call for accountability by the NTIA, we would appreciate more clarity on the "steps" that organizations should take in order to ensure that third parties are likewise accountable. As stated in the *Control* section above, the lack of specificity with regards

---

[22] *SB-1121, California Consumer Privacy Act of 2018*, CALIF. STATE LEGISLATURE (2018), http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121.

[23] "Organizations should be accountable for the use of personal data that has been collected, maintained or used by its systems. As described below in the High-Level Goals for Federal Action section, external accountability should be structured to incentivize risk and outcome-based approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes. Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data." *Developing the Administration's Approach*, *supra* note 6.

to third parties presents a loophole that serves to undermine the stated goals of these principles. We suggest that the NTIA include an obligation for companies to use reasonable care in selecting and monitoring service providers and other third parties in this section.

Finally, while the NTIA should specify in this section that companies will be held accountable by the FTC, we urge the Administration to include other methods of redress. While the FTC has long-served consumers as an important regulator and enforcer, consumers need additional methods of resolution. These Privacy Outcomes do not call for a private right of action or enforcement by state attorneys general. Both are important methods of enforcement, incentivization, and consumer protection and should be included in these principles.

What is Missing from the Privacy Outcomes Section

Unfortunately, the listed Privacy Outcomes fail to include a call for no discrimination or denial of service on the basis of a consumer exercising their privacy preferences and controls.

Privacy should not be a luxury good. Any enunciation of Privacy Outcomes should include a prohibition against any discrimination with regards to the consumer or a denial of service for implementing their privacy choices. Pay-for-privacy schemes could also further exacerbate the untenable and unbalanced relationship between consumers and the companies that continually track them across on- and offline in order to create an intricate dossier of information about them. Any service plan that charges users more for making privacy-conscious choices will disproportionately affect lower-income households. Furthermore, pay-for-privacy plans will also serve to make monthly service plan or product costs less transparent and frustrate consumer efforts to comparison shop. Finally, although some online products and services will inherently lack some functionality if a consumer fully exercises all privacy protections provided, consumers should not be denied service or access on the basis of their personal data and privacy concerns.

B. High-Level Goals for Federal Action

1. Harmonize the Regulatory Landscape[24]

While we agree that harmonization is an important policy goal, too often, a call for harmonization signals a willingness to preempt important state regulations and replace them with a lower set of standards, which would weaken existing protections for many consumers. Strong federal laws should preempt conflicting state laws, particularly if they are weaker. However, states should be allowed to innovate in order to offer stronger protections and to address new threats not known today, because states have more flexibility to respond to emerging privacy and security threats than the federal government. This framework should not pose a significant challenge to companies: they can simply develop consistent practices that meet the highest standard for safety, security, and privacy.

States are uniquely suited to addressing new and emerging threats. For example, following the Equifax data breach, the state legislatures saw a flurry of activity in response. A handful of states removed fees for credit freezes in early 2018.[25] Alabama and South Dakota, the final two states, passed data breach notification laws.[26] And several states, including Alabama, Colorado, Iowa, and Nebraska, passed new data security requirements.[27] The New York State Department of Financial Services extended its tough cybersecurity standards to companies like Equifax,[28] establishing new reporting requirements and oversight procedures.[29] While the federal

---

[24] "While the sectoral system provides strong, focused protections and should be maintained, there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations. We are actively witnessing the production of a patchwork of competing and contradictory baseline laws. This emerging patchwork harms the American economy and fails to improve privacy outcomes for individuals, who may be unaware of what their privacy protections are, and who may not have equal protections, depending on where the user lives. Steps need to be taken to ensure that the regulatory landscape for organizations that process personal data in the United States remains flexible, strong, predictable, and harmonized." *Developing the Administration's Approach*, *supra* note 6.

[25] *See*, *e.g.*, *Credit Freeze & Fraud Alerts*, WASH. STATE OFFICE OF THE ATTORNEY GENERAL, https://www.atg.wa.gov/credit-freeze-fraud-alerts; *Governor Signs AG's Bill to End Credit Freeze Fees* (last visited Nov. 2, 2018); *Governor Signs AG's Bill to End Credit Freeze Fees*, IOWA DEPT. OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL (Apr. 10, 2018), https://www.iowaattorneygeneral.gov/newsroom/reynolds-equifax-credit-freeze-fees/.

[26] David Slaughter, *The Final Two: South Dakota, Alabama Pass Breach Notification Laws*, HR ADVISOR (Apr. 13, 2018), https://hrdailyadvisor.blr.com/2018/04/13/final-two-south-dakota-alabama-pass-breach-notification-laws/.

[27] *Alabama Becomes Final State to Enact Data Breach Notification Law*, PRIVACY & INFO. SECURITY LAW BLOG (Apr. 3, 2018), https://www.huntonprivacyblog.com/2018/04/03/alabama-becomes-final-state-enact-data-breach-notification-law/; David M. Brown, *Colorado Enacts Sweeping Changes to Data Breach Reporting Requirements and Adds New Data Security Requirements*, DATA PRIVACY MONITOR (May 31, 2018), https://www.dataprivacymonitor.com/data-breach-notification-laws/colorado-enacts-sweeping-changes-to-data-breach-reporting-requirements-and-adds-new-data-security-requirements/; *Iowa and Nebraska Enact Information Security Laws*, PRIVACY & INFO. SECURITY LAW BLOG (June 19, 2018), https://www.huntonprivacyblog.com/2018/06/19/iowa-nebraska-enact-information-security-laws/.

[28] 23 NYCRR 201, NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (June 25, 2018), https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/NSText_A_23_NYCRR_201.pdf.

[29] *Id*. at 2-4.

government finally removed fees for credit freezes in May 2018, it has yet to make similar progress in expanding data security protections for consumers following the breach.[30]

Over the past year, states have also passed privacy legislation, reflecting new concerns about consumer control of their own data. Following the Facebook-Cambridge Analytica scandal of March 2018, in which it was revealed that Facebook had shared sensitive information about millions of consumers for political advertising purposes—in nearly all cases without their knowledge[31]—a pending California privacy ballot initiative gained momentum in the state.[32] Within three months, the sponsors pulled the ballot initiative, and Governor Jerry Brown had signed replacement legislation. This new legislation, the California Consumer Protection Act (CCPA), is the most ambitious state privacy law to date.[33]

And in May 2018, Vermont passed a new law requiring data brokers to register with the state, bringing new visibility to these shadowy organizations that collect and sell consumer data.[34] While the law does not provide comprehensive privacy protections, it is an important first step in doing so. It extends security requirements to data brokers, and also requires them to provide information about opportunities to opt-out of the collection or sale of their data.[35] States have pointed the way, but federal policymakers have the opportunity to expand on these protections, and extend them to all Americans. We urge federal policymakers to recognize the states' important role in compelling progress and innovation.

Finally, we appreciate that the NTIA recognizes an important nuance with respect to harmonization, that consumers need particularly stringent protections in certain areas, such as for internet service providers (ISPs). Please see *infra* Section B(3): *Comprehensive Application* for further discussion on this issue.

---

[30] S. 2155, U.S. SENATE (2018), https://www.congress.gov/bill/115th-congress/senate-bill/2155.

[31] Matthew Rosenberg, et al., *How Trump Consultants Exploited the Facebook Data of Millions,* N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[32] Levi Sumagaysay, *Privacy in California: Ballot Measure Qualifies, Bill Advances*, THE MERCURY NEWS (June 26, 2018), https://www.mercurynews.com/2018/06/26/privacy-in-california-ballot-measure-qualifies-bill-advances/

[33] Devin Coldeway, *California Passes Landmark Data Privacy Bill*, TECHCRUNCH (June 28, 2018), https://techcrunch.com/2018/06/28/landmark-california-privacy-bill-heads-to-governors-desk/.

[34] H. 764, VERMONT LEGISLATURE (2018), https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.

[35] AJ Dellinger, *Vermont Passes First-of-its-Kind Law to Regulate Data Brokers*, GIZMODO (May 27, 2018), https://gizmodo.com/vermont-passes-first-of-its-kind-law-to-regulate-data-b-1826359383.

2. Legal Clarity[36]

Legal clarity would be best achieved under a regime in which the FTC is given the ability to issue clarifying rules. Please see *infra* Section B(7): *FTC Enforcement* for more information and *supra* Section A(1): *Risk Management* for our comments regarding how the risk- and harms-based framework introduces a lot of uncertainty for consumers.

3. Comprehensive Application[37]

We support the NTIA's call for comprehensive application; however, we urge the NTIA to support higher requirements for certain industries, such as ISPs. ISPs have unique insight into customer activity because they provide internet service—for which they charge customers a substantial subscription fee—giving them access to a vast amount of data from and about their consumers. While it may be possible for some consumers to take action to reduce their privacy risks once they are online, they have no choice but to use an ISP to access the internet and thus to subject all of their online data to snooping from the ISP. And consumers often have little or no choice over which ISP to use. All of an individual's traffic flows over that internet connection, traffic which can convey very personal information such as personal banking details, presence at home, physical ailments, physical location, race or nationality, religion, and sexual preference.[38] Even when traffic is encrypted, ISPs still know the sites and services their customers use.

In addition to their unique role, ISPs deserve unique treatment due to their status as a necessary utility. Consumers depend on the internet to conduct myriad tasks, including searching for health information, paying bills, finding employment, and accessing state and federal government resources. We support higher requirements for ISPs based on this unique role, the lack of market competition and consumer choice, and their status as a necessary utility. ISPs should be required to get the consumer's opt-in consent for any personal data collection and use outside what is necessary to provide the service and comply with law enforcement.

---

[36] "The ideal end-state would ensure that organizations have clear rules that provide for legal clarity, while enabling flexibility that allows for novel business models and technologies, as well as the means to use a variety of methods to achieve consumer-privacy outcomes. The Administration understands that balancing legal clarity, flexibility, and consumer privacy requires compromise and creative thinking. It is in striking this balance, however, that the United States has been able to maintain international leadership in both innovation and privacy enforcement, and any future action should strive to create a system that to the greatest extent possible maximizes each." *Developing the Administration's Approach*, *supra* note 6.

[37] "Any action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws. The differences between business models and technologies used should be addressed through the application of a risk and outcome-based approach, which would allow for similar data practices in similar context to be treated the same rather than through a fragmented regulatory approach." *Id*.

[38] *See What ISPs Can See*, UPTURN (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

4. Risk and Outcome-Based Approach[39]

As we stated *supra* in Section A(7): *Accountability*, we favor a data policy that pairs substantive controls over process mandates. Without substantive controls, the policy will not sufficiently protect consumers. Please see *supra* Section A(1): *Risk Management* for our feedback on this risk and outcomes-based approach to pressing consumer privacy issues.

5. Interoperability[40]

Consumers Union urges caution when the nation is addressing consumer protection issues through non-democratic instruments like treaties, where those agreements could weaken privacy frameworks. We oppose the use of treaty processes to prohibit or punish nations from adopting laws to protect its people's personal information. While we are sympathetic to concerns about data localization mandates, providing for the free flow of data should not fundamentally nations' ability to safeguard consumer interests.

6. Incentivize Privacy Research[41]

Consumers Union supports the expansion of privacy research.

---

[39] "Instead of creating a compliance model that creates cumbersome red tape—without necessarily achieving measurable privacy protections—the approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes. Risk-based approaches allow organizations the flexibility to balance business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs, when making decisions about how to adopt various privacy practices. Outcome-based approaches also enable innovation in the methods used to achieve privacy goals. Risk and outcome-based approaches have been successfully used in cybersecurity, and can be enforced in a way that balances the needs of organizations to be agile in developing new products, services, and business models with the need to provide privacy protections to their customers, while also ensuring clarity in legal compliance." *Developing the Administration's Approach*, *supra* note 6.

[40] "The growth and advancement of the internet-enabled economy depends on personal information moving seamlessly across borders. However, the Administration recognizes that governments approach consumer privacy differently, creating the need for mechanisms to bridge differences, while ensuring personal data remains protected. The Administration should therefore seek to reduce the friction placed on data flows by developing a regulatory landscape that is consistent with the international norms and frameworks in which the United States participates, such as the APEC Cross-Border Privacy Rules System." *Id*.

[41] "The U.S. Government should encourage more research into, and development of, products and services that improve privacy protections. These technologies and solutions will include measures built into system architectures or product design to mitigate privacy risks, as well as usability features at the user-interface level. These innovations require more research into understanding user preferences, concerns, and difficulties, as well as an understanding of the impact on legal obligations of third parties and the ability of third parties to exercise other rights provided by law. Privacy research will inform the development of standards frameworks, models, methodologies, tools, and products that enhance privacy." *Id*.

7. FTC Enforcement[42]

We strongly agree that, with certain limited exceptions, the FTC is the appropriate agency to oversee consumer privacy and security law, and that the Commission should have the resources, authority, and direction it needs to protect consumers' privacy. However, the FTC is woefully understaffed: the FTC has just over a thousand employees in total, and is tasked with overseeing giants like Google and Facebook.[43] The agency lacks adequate rulemaking authority to properly oversee these companies. Congress should *immediately* allocate sufficient resources to significantly expand the FTC's staff, including: adding technologists at the Bureau of Technology; provide rulemaking authority; and pass clear privacy and security laws, with strong enforcement mechanisms.

The most important reform to improve the Commission's investigation and enforcement processes would be to dramatically expand staffing. The FTC should urge Congress to provide resources to bring on more staff to address litigation needs, provide technical expertise, and enable more frequent and thorough investigations.

Although the economy has doubled in size since the Ronald Reagan administration, the FTC has fewer employees today than it did in at that time.[44] Moreover, especially on privacy and security, other agencies are increasingly abdicating their own responsibilities and deferring authority to the FTC. For example, the Federal Communications Commission supported the Congressional repeal of its broadband privacy rules in order to put the FTC—the "expert" on privacy and security—in charge of policing ISP misbehavior.[45] Similarly, last year the National Highway Traffic and Safety Administration declined to address privacy in its policy framework for automated vehicles, placing responsibility entirely with the FTC.[46]

---

[42] "Given its history of effectiveness, the FTC is the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction, such as HIPAA. It is important to take steps to ensure that the FTC has the necessary resources, clear statutory authority, and direction to enforce consumer privacy laws in a manner that balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate." *Id*.

[43] 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/?utm_term=.a2e56a9b7125.

[44] *Oral Testimony of Commissioner Rebecca Slaughter*, BEFORE THE SUBCOMM. ON DIGITAL COMMERCE & CONSUMER PROT., HOUSE COMM. ON ENERGY & COMMERCE (July 18, 2018), https://democrats-energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-federal-trade-commission-subcommittee-on.

[45] Ajit Pai & Maureen Ohlhausen, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/opinions/no-republicans-didnt-just-strip-away-your-internet-privacy-rights/2017/04/04/73e6d500-18ab-11e7-9887-1a5314b56a08_story.html?utm_term=.b30dabcd3fb5.

[46] Joe Jerome, *NHTSA Automated Vehicle Guidance Punts Privacy to the FTC and Congress*, CTR. FOR DEMOCRACY & TECH. (Sept. 22, 2017), https://cdt.org/blog/nhtsa-automated-vehicles-guidance-punts-privacy-to-the-ftc-and-congress/.

Additionally, several observers have called on the FTC to litigate more cases in order to develop more robust case law on privacy and security (rather than developing norms through negotiated consent decrees).[47] In order to engage in additional litigation to protect consumers, the Commission needs more considerably more attorneys in order to meaningfully contest the practices of deep-pocketed multinational companies. Otherwise, a dictate to take more cases to court will severely hamstring the agency and limit each division to a handful of active cases at any given time.

In addition to privacy and litigation staff, the Commission also needs to substantially expand its technical expertise. The FTC has made important strides in recent years between the establishment of the Chief Technologist position advising the Chairman and the creation of the Office of Technology Research and Investigation (OTECH). Nevertheless, more is needed. OTECH currently only has a handful of technologists to support all five bureaus of the Consumer Protection Bureau; the Bureau of Competition has no analogous office to assist it. Given widespread concerns about concentration and anti-competitive practices in the technology sector, the lack of access to technologists is troubling. The FTC should urge Congress for resources to bring more technologists into the agency, potentially with the aim of developing a full-fledged Bureau of Technology.

Furthermore, in order to fulfill its ever-expanding mission, the Commission should also request Congress to grant it general rulemaking authority under Section 5 to give it the full panoply of tools to address emerging consumer protection threats. Many FTC critics have argued that a reasonableness standard for data security does not give companies sufficient guidance on what practices are required.[48] Similarly, the 11th Circuit in the recent *LabMd* decision held that an order to develop a "reasonably designed" security program was vague and unenforceable.[49] In order to offer more clarity and certainty to companies as to what the law requires, the FTC should have the ability—certainly at least on data security—to engage in Administrative Procedure Act[50] rulemaking.

The FTC currently lacks sufficient remedial tools to fulfill its consumer protection mandate and to deter illegal conduct, and we strongly support additional powers—most notably civil penalty authority—to augment its current authority. Today, when a company commits an actionable privacy or security violation under Section 5 of the FTC Act, the Commission does not have the

---

[47] *E.g.*, David Bahr, *You Down to Reform the FTC—Yea, You Know Me!*, R ST. INST. (Dec. 2, 2017), https://www.rstreet.org/2017/12/07/you-down-to-reform-the-ftc-yea-you-know-me.

[48] Brief for TechFreedom *et al.* as AMICUS CURIAE, FTC V. WYNDHAM WORLDWIDE CORP., 10 F. Supp. 3d 602 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015); Gerard Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673-720 (May 9, 2013), *available at* https://ssrn.com/abstract=2263037.

[49] LABMD, INC. V. FED. TRADE COMM'N, 894 F.3d 1221 (11th Cir. 2018).

[50] *See* 5 U.S.C. §§ 500-504.

ability to obtain penalties from the company. Nor in most cases is restitution an appropriate remedy, as privacy harms or security risks are difficult to quantify and, while possibly substantial in aggregate, may be relatively small in any individual case. The FTC has ordered the disgorgement of ill-gotten gains in some cases,[51] and should expand its use of that authority in lieu of the ability to obtain penalties. However, even in those cases, a company must only cede what it gained directly from its bad behavior, which hardly serves as a sufficient deterrent to others given the relatively small chance of an FTC action. Certainly, the costs of defending an FTC action, the incumbent loss of customer goodwill, and the cost of implementing a compliance program are non-negligible, but in all they are still insufficient to deter rational actors from engaging in unlawful anti-consumer behaviors: the uncertain application of Section 5 in privacy and security matters, along with the relative unlikelihood of enforcement, are hardly outweighed by the weak consequences if they are caught.

The Federal Trade Commission should be granted civil penalty authority for all Section 5 consumer protection matters, and granted comparable authority in any new privacy and security statute. The way that penalties are assessed for violations of trade regulations is, the appropriate model for other FTC penalties. Penalties should be assessed per violation—or per person affected—not based on the number of days on which a violation has occurred, as has been proposed in some legislation. The latter would lead to obviously perverse results—a company could deliberately share or publish to the world all its customer records just for one day, with disastrous results. Nor should the FTC's penalty authority be subject to a hard, monetary cap, as has also been proposed in some legislation. The appropriate penalty for a small business is obviously very different than it should be for a giant company such as Google or Facebook; a cap would only favor the largest companies and most harmful violations, and thus weaken a law's deterrent and retributive effect as to them. Instead, the penalty amount should be reasonably tied to factors such as the nature of the violation, the types of data compromised, the willfulness of the behavior, and the size of a company, as well as its ability to pay.

Section 5 of the FTC Act is not sufficient to ensure the privacy for American consumers deserve and expect.[52] While the Commission's interpretation of Section 5 to mandate reasonable security

---

[51] *Uber Agrees to Pay $20 Million to Settle FTC Charges that it Recruited Prospective Drivers with Exaggerated Earnings Claims*, FED. TRADE COMM'N (Jan. 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/uber-agrees-pay-20-million-settle-ftc-charges-it-recruited. Additionally, we reject the assertion of Commissioner Ohlhausen that disgorgement should be tethered to the amount of consumer harm in any particular case. Rather, the purpose of disgorgement is to deprive a wrongdoer of the fruits of his illegal behavior, not to reward such behavior unless harm can be meaningfully assessed and measured in any particular instance.

[52] Recent research from Forrester shows that consumers are increasingly concerned about how their data is being used online. Greg Sterling, *Survey: Chasm Exists Between Brands and Consumers on Data Privacy*, MARTECH (Apr. 6, 2018), https://martechtoday.com/survey-chasm-exists-between-brands-and-consumers-on-data-privacy-213646. This concern has resulted in individuals trusting fewer brands. *Id.* Additionally, 61 percent of US adults expressed concern about the sharing of their data or online behaviors between companies. *Id.* And an increasing number of consumers (33 percent) block ads when online and use browser do-not-track settings (25 percent). *Id.* Despite these tools, the majority of consumers (61 percent) would like to do more to protect their privacy. Lee

practices sets an appropriate baseline standard, dedicated security legislation would be beneficial for consumers and industry. As companies have challenged (unfortunately, with some success) the FTC's interpretation of Section 5 and enforcement remedies in court, it would be beneficial to articulate a reasonable security mandate in a dedicated statute. Moreover, as some have criticized the FTC reasonableness standard as not offering sufficient notice to businesses about appropriate security practices and procedures,[53] the FTC should propose a dedicated statute to give the Commission rulemaking authority to offer greater clarity and certainty over time as to what reasonable security entails.

Finally, the Federal Trade Commission needs dramatically more resources to achieve its consumer protection mission and should include these resources in its next budget request. The Commission currently has too few people to bring sufficient cases to effectively deter illegal conduct, and modern internet platforms that host more and more online commerce and advertising do not themselves have sufficient incentives to police their platforms for bad conduct. In addition to Congress dedicating substantially greater funds to augment the FTC's capacity, any new privacy and security statute should also empower state attorneys general to bring enforcement actions in order to supplement the Commission's own work on behalf of consumers.

8. Scalability[54]

For companies to be sufficiently incentivized to protect consumer data and honor consumer preferences, fines should be proportionate to the scale of the wrongdoing, ability to pay, sensitivity of the data compromised. Although we cautioned against the use of a balancing test for the scope of privacy obligations earlier in these comments, a balancing approach would work well in the assessment of penalties for wrongdoing. However, it is worth noting that some very

---

Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[53] Gerard Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673-720 (May 9, 2013), *available at* https://ssrn.com/abstract=2263037.

[54] "The Administration should ensure that the proverbial sticks used to incentivize strong consumer privacy outcomes are deployed in proportion to the scale and scope of the information an organization is handling. In general, 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. Similarly, there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations. Just as organizations should employ outcome-based approaches when developing privacy protections for their customers, the government should do the same with its approach to privacy enforcement and compliance." *Developing the Administration's Approach*, *supra* note 6.

small companies could have very expansive, sensitive data. For instance, when Instagram[55] and Spokeo[56] were new companies they only had around 10 or less employees and yet had access to large swaths of sensitive data. We urge the NTIA to specifically call out the potential for expansive data collection (and negative consequences) from even very small companies' data practices.

[55] Instagram began and ran with a small staff for years before it ballooned to its current size. Eric Markowitz, *How Instagram Grew from FourSquare Knock-Off to a $1 Billion Photo Empire*, INC. (Apr. 10, 2012), https://www.inc.com/eric-markowitz/life-and-times-of-instagram-the-complete-original-story.html.

[56] Spokeo was started with a staff of four, but now currently employs hundreds of people. David Lazarus, *Spokeo website gathers details on everyone, except its founder*, SUN SENTINEL (July 2, 2010), https://www.sun-sentinel.com/business/fl-xpm-2010-07-02-fl-people-search-0628-20100701-story.html.

Thank you for the opportunity to respond to your request for comment on the administration's approach to consumer privacy.

Sincerely,

Katie McInnis
Policy Counsel
Consumers Union
1101 17th Street NW, Suite 500
Washington, DC 20036

Maureen Mahoney
Policy Analyst
Consumers Union
1535 Mission Street
San Francisco, CA 94103