Comments to the National Telecommunications and Information Administration

From Consumer Federation of America, Consumer Action, the National Consumers League, and Privacy Rights Clearinghouse

Docket No. 1808211780-8780-01

November 9, 2018

Consumer Federation of America[1], Consumer Action[2], the National Consumers League[3], and Privacy Rights Clearinghouse[4] welcome the opportunity to comment on the proposal[5] from the National Telecommunications and Information Administration (NTIA) to "advance consumer privacy while protecting prosperity and innovation." In describing the United States' "leadership" in developing privacy norms, the NTIA refers to the Fair Information Practice Principles,[6] which state:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

These principles have been implemented in the federal government's data practices, but they have never been enacted in a comprehensive manner to govern commercial data practices. The United States has *not* led the way in this area; in fact, it has fallen far behind other parts of the world. For instance,

[1] Consumer Federation of America (CFA) is a nonprofit association of consumer organizations established in 1968 to advance consumers' interests through research, education and advocacy.

[2] Using multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers low- and moderate-income, limited-English-speaking, and other underrepresented consumers nationwide to financially prosper through education and advocacy.

[3] The National Consumers League is a private, nonprofit advocacy group representing consumers on marketplace and workplace issues.

[4] Privacy Rights Clearinghouse is a 501(c)(3) nonprofit organization protecting privacy for all by empowering individuals and advocating for positive change.

[5] Federal Register Vol. 83, No 187 (September 26, 2018), notice and request for comments, https://www.gpo.gov/fdsys/pkg/FR-2018-09-26/pdf/2018-20941.pdf.

[6] The Health, Education, and Welfare Advisory Committee on Automated Data Systems, created in 1972, recommended the enactment of a "Code of Fair Information Practice." This became the foundation for guiding the federal government's data practices. *See* https://www.epic.org/privacy/consumer/code_fair_info.html; the Committee's full report, "Records, Computers and the Rights of Citizens" (July 1973) is available at https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

recognizing that privacy is a fundamental human right, the European Union has had data protection legislation in place since 1995, and in May 2018 a new General Data Protection Regulation (GDPR) took effect, updating and strengthening Europeans' rights and enforcement powers[7]. The NTIA proposal, with its risk-management rather than rights-based approach, does not provide an acceptable roadmap for the kind of privacy protection that Americans need and that would help achieve the legal clarity and interoperability that the administration seeks to foster.

Comments on Privacy Outcomes

The NTIA proposes a set of desired privacy outcomes: transparency, control, reasonable minimization, security, access and correction, risk management, and accountability. These track, to a certain extent, some of the widely-respected principles in the Privacy Framework of the Organization for Economic Cooperation and Development (OECD)[8]:

> **Collection Limitation Principle**
>
> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> **Data Quality Principle**
>
> Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> **Purpose Specification Principle**
>
> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> **Use Limitation Principle**
>
> Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
> a) with the consent of the data subject; or
> b) by the authority of law.
>
> **Security Safeguards Principle**
>
> Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

[7] Information about the GDPR and other EU data protections is available at https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.
[8] *See* http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

Individuals should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
b) to have communicated to them, data relating to them
    i. within a reasonable time;
    ii. at a charge, if any, that is not excessive;
    iii. in a reasonable manner; and
    iv. in a form that is readily intelligible to them;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

We will refer to these OECD principles as we discuss the outcomes that the NTIA proposes.

Transparency

Transparency is important value, as reflected in the OECD openness principle. But that principle is not meant to be implemented in isolation; it is not enough to simply be transparent about one's privacy practices without taking into account other essential principles such as collection limitation, data quality, purpose specification, and use limitation.

The NTIA outcomes do not appear to be predicated on the notion that public policy should place any limits on the collection of personal data, that such collection be done by lawful and fair means, and, where appropriate, with the knowledge or consent of the data subject. While the outcomes call for user control and data minimization, they fall far short of effectively addressing those issues from the perspective of the individuals whose personal information is involved, as we will discuss later.

The concept of purpose specification is not adequately captured in the statement that "Users should be able to easily understand how an organization collects, stores, uses and shares their personal information" because it does not place any affirmative duty on the organization to describe its data practices, let alone be specific about the purposes for which the data is collected, used or shared. The

related principle of limiting use to those specified purposes is nowhere to be found in the outcomes, nor is there any mention of ensuring data quality.

We agree that lengthy notices describing companies' privacy programs do not lead individuals to understand their data practices. Companies should clearly and accurately explain their data practices, in plain language, and make that information easily accessible. A requirement for simple, standardized notices might be helpful to increase public awareness about how personal data is gleaned and used, compare companies' data practices, and monitor companies' behavior. It is not reasonable, however, to expect that as an outcome of better notices individuals will "understand" companies' data practices, since even improving the quality, format and availability of this information cannot guaranty that individuals will read or comprehend it. Furthermore, that places the burden on individuals to protect their privacy and security rather on companies to align their data practices with fair information principles.

Control

Many studies[9] have shown that Americans feel they lack control of their personal information, and to a large extent they are correct. With some limited exceptions, companies can collect, store, share, sell, and use individuals' personal data as they see fit. As personal information has increasingly become a valuable form of currency in the marketplace, there is little incentive to give individuals greater say in this regard – or to accept limits set by public policy.

The NTIA describes an outcome in which "Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations."[10] We have several concerns about this statement. First, it is not clear what the NTIA means by "control," but this again seems to imply that it's up to individuals to protect themselves, to the extent they can, from unwanted data practices (though in describing the overall outcome it hopes will emerge from this initiative, the NTIA acknowledges that having "a reasonably informed user, empowered to meaningfully express privacy preferences" is not enough in some cases, "particularly in business contexts in which relying on user intervention may be insufficient to manage risks" and calls for "products and services that are inherently designed with appropriate privacy protections"[11]).

Second, the use of the word "reasonable" raises the question of who decides what is reasonable. Again, since OECD principles such as collection limitation, purpose specification, and use limitation are not

---

[9] Surveys by the Pew Research Center, summarized in "The state of privacy in post-Snowden America" (September 21, 2016), show that very few Americans are confident that organizations, including businesses, will keep their personal information private and secure; 91% agree that consumers have lost control over the personal information that companies collect; 47% said they were not sure what information is collected about them or how it is used; 65% said that it is very important to them what information is collected about them and 74% said it is very important to them how that information is used; and the majority of Americans favor additional legal protections against abuses of their data, with 68% believing that current laws are not good enough to protect people's privacy online. Available at http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/. The NTIA's own survey data indicates that concerns about privacy and security deter cause many internet users to hold back on their online activities, *see* NTIA blog, "Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds" (August 20. 2018), available at https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

[10] *Supra* at 48601.

[11] *Id*.

invoked here, it appears to be left to the companies, not to public policy, to decide what controls, if any, they deem reasonable to provide. It is hard to imagine how this approach could lead to strong privacy protections or the legal clarity and interoperability that the NTIA seeks. The vague language about taking into consideration factors such as users' expectations and the sensitivity of the data (again, a subjective qualification) does not help. The Fair Information Practice Principles that the NTIA cites as demonstrating the United States' leadership in privacy provide more clear and straightforward guidance; for instance in stating that "There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent."

Another troubling qualifier is the phrase "the personal information they provide to organizations." Companies may obtain individuals' personal information in many different ways. Individuals provide certain personal information directly to companies when they are making purchases and setting up accounts, but companies may also obtain their personal information from data brokers (which collect that information from third parties, not directly from individuals), affiliates, business partners, and other sources. When consumers visit websites, personal information can be collected by the site operators and by others, such as the internet service providers that connect them to those sites and "marketing clouds" that collect, analyze and sell that information for marketing purposes. When individuals use mobile devices, their locations and other personal information may be gleaned by their carriers, internet service providers, app providers, and others. When they use internet-connected devices such as smart TVs and energy meters, personal information can be collected by the manufacturers and service providers. License plate readers and facial recognition systems collect personal information. In these and many other instances individuals may not be consciously "providing" their personal information to anyone[12].

In our view, the best way to achieve an outcome in which individuals have meaningful control of their personal information is to adopt public policy that requires their data to be treated in accordance with the basic fair information principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, individual participation, and accountability. The right to data portability, which the NTIA does not raise here and which is one of the important provisions of the GDPR, is also helpful to give individuals real data control. Furthermore, we believe that it is essential to prohibit terms of service that require individuals to waive their rights, financial incentives in exchange for forgoing their rights, and forced arbitration to resolve disputes. These practices are unfair and contrary to the notion of "user-centric" privacy outcomes.

Reasonable Minimization

Data minimization is reflected in the OECD principle of data quality (Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date) and also in the purpose specification and use limitation

[12] A fundamental question that the NTIA fails to address is: what is "personal information?" We believe that the definition must be sufficiently broad to include any information that is related to or can be reasonably linked to the individual, not only traditional identifiers such as names, addresses, phone numbers, and account numbers and the like, but also biometric data and persistent identifiers such as device identifiers, MAC addresses, and static IP addresses. *See*, for instance, definition of personal information in California Consumer Privacy Act, AB 375, Section 3, 1798.140 (o) (1), at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

principles. Minimizing the amount and types of data that a company collects, sharing it only as needed for the purposes for which it is intended to be used, and retaining it only for as long as needed can obviously help reduce the risk of a "privacy harm." But data quality also ensures that it is "good" for the purposes for which it will be used and provides the outcome that it should for the individual.

Security

The non-stop stream of data breaches that we are experiencing in the United States is very disheartening. Despite the NTIA's work to help develop and promote strong industry standards, efforts to increase business awareness about how to secure data and the importance of doing so, and the expenses and reputational harm that breached entities often incur, there does not appear to be enough incentive to take data security seriously. Breaches are considered a "cost of doing business." We hear over and over again that there can never be "perfect security." Perhaps not, but incidents such as the Equifax breach, in which there does not seem to have been any system in place to ensure that a known security vulnerability was patched, are simply inexcusable.[13]

The NTIA does not present any new concepts for how to achieve an outcome in which individuals can be assured that their personal information will be adequately secured. We believe that this is another area that must be addressed through public policy. One recommendation is to strengthen the ability of the Federal Trade Commission (FTC) to enforce security requirements by eliminating its jurisdictional constraints, providing it with rulemaking authority, empowering it to levy civil penalties, and providing it with more staff and other resources.[14] The United States could also create a separate, independent Data Protection Authority, as exists in many other countries, which would have the mandate and capacity to provide guidance to businesses, educate the public, examine issues, investigate possible violations of law, and bring effective enforcement actions when necessary.

Another recommendation is to institute strict liability for inadequate security[15]. Furthermore, a requirement to make individuals "whole" in the event of a breach and empowering them to take legal action when their security rights are violated would provide an additional incentive for companies to secure the personal data they hold.

Access and Correction

The ability of individuals to access, correct and delete their data is reflected in the OECD principle on individual participation. It is essential for data quality and portability. If by saying that individuals should have "qualified" access and abilities in this regard the NTIA means that there should be reasonable means to verify the individual making the request, we agree. We also believe that it is appropriate for an

[13] See Lily Hay Newman, Wired, "Equifax Officially has No Excuse" (September 14, 2017), available at https://www.wired.com/story/equifax-breach-no-excuse/.

[14] *See* comments from CFA to the FTC regarding its remedial authority to deter unfair and deceptive conduct in privacy and security data matters (August 20, 2018), available at https://consumerfed.org/wp-content/uploads/2018/08/cfa-comments-regarding-ftc-remedial-authority-to-deter-unfair-deceptive-conduct.pdf.

[15] For example, the Data Breach Prevention and Compensation Act of 2018 would impose civil penalties for data breaches at credit reporting agencies, text available at https://www.congress.gov/115/bills/s2289/BILLS-115s2289is.pdf. *See* also Benjamin C. Dean, "Strict Liability and the Internet of Things" (April 2018), Center for Democracy & Technology, available at https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

organization to decline a request to delete data when it is necessary to retain it for the specified purpose (assuming that it has been obtained in line with the collection limitation principle and is used pursuant to the use limitation principle).

We are not sure, however, what is meant by "given the context of the data flow" or "appropriate to the risk of privacy harm." From our perspective, privacy is a fundamental human right, and individuals' ability to access, correct and delete their personal information flows from that right. It is not contingent on whether there is a risk of harm.

Risk Management

This "outcome" goes to the heart of our concerns about this administration's approach to privacy. Privacy is a right to be respected, not a risk to be managed. A violation of an individual's privacy rights is in itself a "harm." Users should expect organizations will align their data practices with the basic fair information principles and other public policy requirements that we as a society agree to set. Innovation in business models should occur within that framework and "privacy tools" should serve that end.

Accountability

Organizations should be accountable for complying with the requirements that public policy sets concerning data privacy and security. "Privacy by design" is integral to achieving this outcome. Another important component of accountability is for organizations to ensure, through contracts and auditing, that third parties are held to clear, specific requirements for their use, storage, processing, and sharing of personal data made available to them[16]. Accountability should begin at the top, with the board of directors and senior management of an organization. It is also important to designate specific individuals within an organization to be responsible for ensuring that privacy and security protocols are followed.

<u>High-level Goals for Federal Action</u>

We believe that the primary goal of any federal action concerning privacy and security should be to enact comprehensive baseline legislation that will provide Americans with strong data protection and redress. Our organizations have joined other consumer, civil rights and privacy groups in proposing "Public Interest Privacy Legislation Principles"[17] which at a high level provide a foundation for federal action.

Our comments on the NTIA proposed high-level goals follow.

---

[16] For example, Facebook's apparent failure to adequately control and monitor third party access and use of members' personal information came into sharp focus in the Cambridge Analytica scandal, *see* Elizabeth Dwoskin and Tony Roman, Washington Post, "Facebook's rules of accessing user data lured more than just Cambridge Analytica" (March 19, 2018), available at https://www.washingtonpost.com/business/economy/facebooks-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/31f6979c-658e-43d6-a71f-afdd8bf1308b_story.html?utm_term=.617227b99bca.

[17] These principles are appended to this document and will be available on CFA's website on November 13, 2018 at https://consumerfed.org/wp-content/uploads/2018/11/public-interest-privacy-principles.pdf.

Harmonize the regulatory landscape

There has always been a multi-faceted approach to data privacy and security in the United States. At the federal level, we have a variety of sector-specific laws such as those pertaining to communications services, health providers, financial institutions, and companies that offer online products and services to children. States also play an important role in protecting individuals' privacy and security. Every state has now implemented data breach notification requirements. States have enacted many other laws and regulations related to personal data, including biometric data[18], information collected about shoppers in supermarket loyalty programs[19], data brokers[20], the solicitation and use of Social Security numbers[21], data security[22], and the right to know what information is collected about individuals online.[23] Some cities have acted to protect residents' broadband privacy[24].

The NTIA states that this "patchwork" of laws "harms the American economy and fails to improve privacy outcomes for individuals…" without providing any evidence for either claim. We believe that governments at all levels should play a role in protecting and enforcing Americans' privacy rights. The federal government should set strong, minimum standards, and the states, which are more flexible and quicker to act, should be able to enact more stringent requirements and address emerging issues as needed. "Harmonization" at the federal level that sets low standards, preempts the states, and blocks individuals from enforcing their rights through forced binding arbitration and by prohibiting class actions may provide "predictability" but does not serve the public interest.

Legal clarity while maintaining the flexibility to innovate

Businesses have always innovated within the parameters set by public policy; for instance, in developing safe cars, energy-efficient appliances, and new medications. The laws and regulations that apply to these products provide the legal clarity that guides their production and sale.

Federal data protection legislation based on all fair information principles and that provides for appropriate rulemaking and strong enforcement would provide clarity about organizations' responsibilities for privacy and security while at the same time enabling creativity and innovation to flourish. As systems for collecting, analyzing and using individuals' personal information become ever-more complex, it is crucial for such legislation to address the fundamental fairness of and transparency

---

[18] *See* Texas Business and Commerce Code §503.001, at https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html.

[19] *See* California Title 14.B. 1749.60-1749.66, at http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.4B.&part=4.&chapter=&article

[20] *See* Vermont H. 764 at https://legislature.vermont.gov/assets/Documents/2018/Docs/BILLS/H-0764/H-0764%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf.

[21] *See* Kansas Stat. §75-3520, http://www.kslegislature.org/li_2016/m/statute/075_000_0000_chapter/075_035_0000_article/075_035_0020_section/075_035_0020_k.pdf.

[22] *See* Massachusetts 201 CMR 17.00, https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf.

[23] *See* Nevada 603A.300-360, https://www.leg.state.nv.us/NRS/NRS-603A.html#NRS603ASec220.

[24] *See* City of Seattle, Washington ITD Director's Rule 2017-01, http://www.seattle.gov/tech/about/policies-and-directors-rules.

regarding automated decision-making in order to prevent unfair discrimination and protect equal opportunity.

Employ a risk and outcome-based approach

Again, we believe that the NTIA is wrong to call for an approach to privacy regulations based on "risk modeling" rather than a compliance model based on fair information principles. The NTIA does not define the privacy "harm" that organizations should avoid "risking." We know that some in industry are calling for enforcement of a federal privacy law only when there is a "concrete harm to individuals"[25] – again, without defining what that is.

In our view, harm is not limited to financial loss. As we state in the "Public Interest Privacy Legislation Principles," privacy violations may 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. We believe that legislation should avoid requiring a showing of a monetary loss or other tangible harm, and make clear that the invasion of privacy itself is a concrete and individualized injury.

Interoperability

The U.S. Department of Commerce has been struggling for years with the issue of how to help facilitate cross-border commerce, especially in the internet-enabled economy, when our privacy laws are deemed inadequate by governments in major trading blocs such as the European Union. First the Safe Harbor agreement was invalidated[26] and now its replacement, the Privacy Shield, is in peril[27]. The NTIA cites the APEC Cross-Border Privacy Rules System as a model to "reduce the friction placed on data flows." The APEC rules are not as strong as the GDPR, however. Since US companies operating in Europe are required to comply with the GDPR, we are perplexed as to why the NTIA is not calling for the obvious solution to the interoperability issue: enacting federal legislation that provides strong data protection equivalent to that of the GDPR.

Incentivize privacy research

We support the encouragement of research into, and the development of, products and services that would help organizations comply with privacy requirements and help individuals exert their privacy rights. We believe, however, that many in industry already have a sophisticated understanding of human behavior and are using it to manipulate individuals to make the least privacy-protective

[25] For example, *see* the U.S. Chamber of Commerce Privacy Principles, available at https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.
[26] Courtney M. Bowman, Proskauer Privacy Blog, "US-EU Safe Harbor Invalidated – What Now?" (October 26, 2015), available at https://privacylaw.proskauer.com/2015/10/articles/european-union/us-eu-safe-harbor-invalidated-what-now/.
[27] Natasha Lomas, Techcrunch.com, "EU parliament calls for Privacy Shield to be pulled until US complies," (July 5, 2018), available at https://techcrunch.com/2018/07/05/eu-parliament-calls-for-privacy-shield-to-be-pulled-until-us-complies/.

choices.[28] To the extent that the privacy default is changed by public policy to be more privacy-protective, much of the burden on individuals to protect themselves can be alleviated.

FTC enforcement

The FTC is not and should not be the only agency to enforce consumer privacy. The Federal Communications Commission, the Department of Health and Human Services, the Department of Transportation, the financial regulators – even the Consumer Product Safety Commission, with regard to the safety and security of internet-connected devices[29] – all have important roles to play in protecting individuals' privacy and security. We agree that for the entities over which the FTC has jurisdiction, the agency needs adequate resources, clear statutory authority, and direction to enforce privacy laws. That would include, in our view, rulemaking authority and the ability to issue civil penalties.

As we noted before, the US might be well-served, however, to create a Data Protection Authority with broad authority and enforcement capabilities. This agency could work in cooperation with sectoral regulators and provide overarching coordination and cohesiveness to the federal government's approach to privacy. It could also work with the states to encourage sharing best practices in regulating privacy and security, which would promote greater harmonization of public policies at that level.

Scalability

Even businesses that employ a small number of employees can process vast amounts of data. Rather than scaling responsibility by the size of a business, we believe that governments should have a range of options to consider when they enforce privacy rules. For instance, the GDPR provides for a scale of monetary penalties and EU data protection authorities can also issue warnings in lieu of fines. Enforcement must be meaningful, however; the current constraints on the FTC, which can only seek civil penalties in the event that a company violates an order, and the "right to cure" provisions[30] in the new California Consumer Privacy Protection Act, are concerning because they give companies a free "bite of the apple" to violate individuals' privacy rights without incurring any penalties.

Conclusion

In conclusion, we believe that the goal of federal action on data protection should be the adoption of public policy that requires individuals' personal data to be treated in accordance with the basic fair information principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, individual participation, and accountability. The outcomes should be strong, meaningful, and comprehensive protections to preserve civil rights, prevent unlawful discrimination, and advance equal opportunity. Data protection rights must be enforceable by governments and individuals and provide strong redress. Furthermore, federal action should not prevent the states from implementing and enforcing stronger privacy protections.

---

[28] See Norwegian Consumer Council report, "Deceived by Design" (June 27, 2018), available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[29] See CFA testimony to the Consumer Product Safety Commission on "The Internet of Things and Consumer Product Hazards" (May 2, 2018), available at https://consumerfed.org/wp-content/uploads/2018/05/cfa-testimony-to-cpsc-regarding-internet-of-things.pdf.

[30] *Supra*, 1798.150 and 1798.155.

The harm-based approach advocated by the NTIA discounts the role of privacy in important American values such as dignity, liberty, and equality. We regret that it does not help to advance the privacy debate in the United States or to achieve the legal clarity and interoperability that the administration seeks to foster. We will continue to call for strong data protection rights for all Americans and welcome the opportunity to work with those in government and business who share that goal.

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,[31] people think they lack control over their data,[32] want government to do more to protect them,[33] and distrust social media platforms.[34]

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[35] (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across 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.

---

[31] *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.
[32] 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.
[33] 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.
[34] *Id.*
[35] 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.

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