CENTER FOR DIGITAL DEMOCRACY

November 9, 2018

David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and
Information Administration
United States Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

By Electronic Mail

Comments of the Center for Digital Democracy
To
The National Telecommunications and Information Administration
On
"Developing the Administration's Approach to Consumer Privacy"
Docket No. 180821780-8780-01

Dear Assistant Secretary Redl:

The Center for Digital Democracy, one of the leading U.S. nonprofit organizations focused on privacy and consumer protection in the digital era, respectfully submits the following comments.[1] We appreciate the National Telecommunications and Information Administration's (NTIA) effort and its stated goal to advance consumer privacy in the United States[2].

Focus on Privacy Outcomes Useful, but Framing of Outcomes is too Narrow

The NTIA proposal aims to focus our attention on policy outcomes. It suggests that, instead of using a principle-based approach, we focus on "outcomes of organizational practices, rather

[1] https://www.democraticmedia.org/
[2] https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy; https://www.federalregister.gov/documents/2018/10/11/2018-22041/developing-the-administrations-approach-to-consumer-privacy (extending deadline for comment)

than on dictating what those practices should be." While we welcome a focus on outcomes, the NTIA proposal unfortunately fails to sufficiently discuss and define these desired outcomes. We believe it would be useful to elaborate on such outcomes further. Without an understanding of the outcomes that we would like to achieve via legislation, it is doubtful that we will identify the appropriate policy interventions, or that the entities collecting, using and sharing data will be held accountable. Moreover, progress will be difficult to gauge.

The NTIA's proposal briefly states that "the desired outcome is a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections…." Undoubtedly, an informed and empowered citizen is an important goal, as are privacy-friendly products and services. However, the primary outcome that privacy legislation should ultimately achieve must be the protection of people's privacy. Similarly, the stated list of desired outcomes of transparency, control, reasonable minimization, security, access and corrections, risk management, and accountability are not really privacy outcomes. They are restatements of a privacy self-management regime, as we discuss below. We need to explore the meaning of privacy, its definitions and associated harms. There are, of course, a multitude of definitions of privacy. In the age of predictive and classifying analytics, however, it is particularly important to elaborate on those definitions and to consider a broad range of privacy harms. It is critical to consider those definitions and harms in order to inform policy decision-making and any future legislation.

Among the various harms that have been identified, chief among them, we suggest, are identification harms (risks of identity theft, re-identification and sensitive inferences), discrimination harms (inequities in the distribution of benefits and risks of exclusion), as well as exploitation harms (personal data as commodity and risks to the vulnerable).[3] These harms highlight the distributive nature of privacy harms. CDD believes that a legislative goal must not only be to reduce privacy harms, but also to ensure that "privacy benefits are fairly allocated."[4] Many privacy violations that result in pernicious forms of profiling and discrimination, therefore, are harmful not just to the individual but also to groups and communities, particularly those with already diminished life chances, and to society at large. Policy remedies must consider and be effective in addressing the inequities in the distribution of privacy benefits and harms.

CDD urges NTIA to broaden the debate on policy outcomes. NTIA should explore the full range of privacy outcomes we want to advance, and which policy interventions might be best suited for them.

---

[3] For a detail discussion see Popescu, M., Baruh, L., Messaris, P., & Humphreys, L. (2017). Consumer surveillance and distributive privacy harms in the age of big data. In Digital media. Transformations in human communication (2nd ed., pp. 313-327). New York: Peter Lang.

[4] Ibid., p. 7

Legislation Must Also Focus on Outputs of Data Processing

In addition to considering the range of privacy harms that legislation ought to address, we would like to highlight one other area where we believe legislation would benefit from a different approach: the scope of legislation with regard to personal data. Since we are concerned with the outcomes of data practices and not so much with the data itself, we also urge NTIA to abandon the narrow focus on personal data. Both the risk of re-identification and of inferring sensitive attributes from non-sensitive data are becoming increasingly common in the age of big data.[5] Importantly, while many inferences can be drawn from an individual's personal data, "third party personal data, anonymized data, and other forms of non-personal data can also be used to develop inferences and profiles."[6] The process of drawing inferences can be done without the need of identifiability; only when the results are applied to a person is identifiability relevant again. Thus, individual privacy rights (such as access or deletion rights) can only be exercised *after* "inferences or profiles based on anonymized, non-personal, or third party data have been applied at an individual level." A large aspect of corporate data practices thus may escape accountability. So, as NTIA suggests, rather than focus on the data inputs (whether data is personal, de-identified, anonymized, aggregated, sensitive or not), the risks of big data classifying and predictive analytics requires us to focus on the "outputs of data processing", such as inferences or decisions and other data uses. [7]

Instead of relying on Privacy Self-Management, We Need to Implement Additional Methods to Achieve Desired Outcomes

NTIA's stated desired outcomes of transparency, control, reasonable minimization, security, access and corrections, risk management, and accountability are not really privacy outcomes. Instead, they are a re-statement of the all-too-familiar privacy self-management paradigm. Instead of notice, it proposes "transparency"; instead of consent, it now says "control"; rather than listing purpose limitation, it asks only for "reasonable minimization; "access and correction," as well as "accountability," remain the same. The sole new addition is "risk management," which, indeed, is the "core of this Administration's approach," according to NTIA. As is common with privacy self-management models, the NTIA proposal fails to state how data may be used.

NTIA's proposal fails to elaborate on the approach of a "risk-management" regime. Key to such a process is to identify and agree on the risks that such a process ought to manage. While the proposal lists many important business and economic risks, such as threats to the ability to innovate, interoperability, harmony of the regulatory landscape, and legal clarity, it does not do so with regard to privacy risks and harms. Regardless, any privacy risk-management approach

[5] Ibid., p. 10-11

[6] Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (September 13, 2018). Columbia Business Law Review, Forthcoming . Available at SSRN: https://ssrn.com/abstract=3248829

[7] Ibid. p.56

must define risks broadly. We urge NTIA to develop, perhaps in cooperation with its European colleagues, methodologies to assess the human rights, social, economic and ethical impacts of the use of algorithms in modern data processing.[8] This broader view of risk management would not only focus on the risks to individual privacy, but would also consider group privacy harms and their impact on the advancement of other values, such as equity, fairness, community, competition, efficiency and innovation. These impact assessments should be required for companies who come under special scrutiny for engaging in high-risk data practices. A dedicated data protection agency must provide oversight over these assessments. It would be in a much better position to assess societal risks than the very companies that create those risks.

The problems and limitations of a privacy self-management model have been well documented.[9] Cognitive and structural problems are numerous. Moreover, data analytics undermines the notion that an individual can have control over data that pertains to her. Profiles and inferences are based on data that are derived from other individuals who have consented, on aggregated data or anonymized data, and are out of reach for the individual under a privacy self-management regime. Without one's knowledge or participation, classifying and predictive analytics may still draw inferences about individuals. These can result in injurious privacy violations such as profiling and discrimination, which are ultimately harmful not just to the individual, but also to groups and communities, particularly those with already diminished life chances.

Privacy self-management alone is not enough as a policy solution. Instead of advancing the cause of privacy, the only outcome such a model seems to produce is a dominant paradigm that suggests that policy solutions must be centered on individual action, and that privacy is an individual, commodified good that can and should be traded for other goods.[10] CDD rejects that view.

CDD Proposes a Set of Principles that Aim to Safeguard Privacy Rights, Advance Fair and Equitable Outcomes, Limit Corporate Practices and Ensure Government Enforcement

---

[8] Alessandro Montelero, *AI and Big Data: A blueprint for human rights, social and ethical impact assessment*, Computer Law & Security Review, Volume 34, Issue 4, August 2018, Published by Elsevier Ltd., under the CCBY-NC-ND license,
https://www.sciencedirect.com/science/article/pii/S0267364918302012

[9] See for example, Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard LawReview, 126, 1880-1902;
Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 44-75). Cambridge: Cambridge University Press

[10] Hull, G., *Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data,* Ethics and Information Technology (2015) 17:89–101; DOI 10.1007/s10676-015-9363-z

We are alarmed by the increasingly intrusive and pervasive nature of commercial surveillance, which has the effect of controlling consumers' and citizens' behaviors, thoughts, and attitudes, and which sorts and tracks us as "winners" and "losers." Today's commercial practices have grown over the past decades unencumbered by regulatory constraints, and increasingly threaten the American ideals of self-determination, fairness, justice and equal opportunity. It is high time to address these developments. We are proposing a set of principles (attached) that ought to be considered when developing privacy legislation.[11] Such legislation must

- set the scope of baseline legislation broadly and not preempt stronger legislation;
- grant not only basic rights to individuals and groups regarding data about them, but also
- advance equitable, fair and just uses of data (i.e., it must place limits on certain data uses and safeguard equitable, fair and just outcomes);
- bring about real changes in corporate practices (i.e., set limits and legal obligation to those managing data and require accountability);
- should be consequential and aim to level the playing field (i.e., give government at all levels significant and meaningful enforcement authority to protect individual and common interests vis-à-vis powerful commercial entities and give individuals legal remedies).

In addition to CDD's principles, we also support a set of Public Interest Privacy Legislation Principles (attached) proposed by a broad coalition of civil rights, consumer, and privacy organizations.

Respectfully,

Katharina Kopp, Ph.D.
Deputy Director
Center for Digital Democracy
1875 K Street NW, 4th floor
Washington, DC 20036

[11] https://www.democraticmedia.org/blog/center-digital-democracys-principles-us-privacy-legislation

Center for Digital Democracy's Principles for U.S. Privacy Legislation

Protect Privacy Rights,
Advance Fair and Equitable Outcomes,
Limit Corporate Practices and
Ensure Government Leadership and Enforcement

The Center for Digital Democracy provides the following recommendations for comprehensive baseline Federal privacy legislation. We are building on our expertise addressing digital marketplace developments for more than two decades, including work leading to the enactment of the 1998 Children's Online Privacy Protection Act--the only federal online privacy law in the United States. Our recommendations are also informed by our long-standing trans-Atlantic work with consumer and privacy advocates in Europe, as well as the General Data Protection Regulation.

We are alarmed by the increasingly intrusive and pervasive nature of commercial surveillance, which has the effect of controlling consumers' and citizens' behaviors, thoughts, and attitudes, and which sorts and tracks us as "winners" and "losers." Today's commercial practices have grown over the past decades unencumbered by regulatory constraints, and increasingly threaten the American ideals of self-determination, fairness, justice and equal opportunity. It is now time to address these developments: to grant basic rights to individuals and groups regarding data about them and how those data are used; to put limits on certain commercial data practices; and to strengthen our government to step in and protect our individual and common interests vis-à-vis powerful commercial entities.

We call on legislators to consider the following principles:

1) **Privacy protections should be broad: Set the scope of baseline legislation broadly and do not preempt stronger legislation**
   Pervasive commercial surveillance practices know no limits, so legislation aiming to curtail negative practices should
   a) address the full digital data life-cycle (collection, use, sharing, storage, on- and off-line) and cover all private entities' public and private data processing, including nonprofits;
   b) include all data derived from individuals, including personal information, inferred information, as well as aggregate and de-identified data;
   c) apply all Fair Information Practice Principles (FIPPs) as a comprehensive baseline, including the principles of collection and use limitation, purpose specification, access and correction rights, accountability, data quality, and confidentiality/security; and require fairness in all data practices.
   d) allow existing stronger federal legislation to prevail and let states continue to advance innovative legislation.

2) **Individual privacy should be safeguarded: Give individuals rights to control the information about them**
    a) Building on FIPPs, individuals ought to have basic rights, including the right to
        - transparency and explanation
        - access
        - rectification
        - erasure
        - object and restrict
        - portability
        - use privacy-enhancing technologies, including encryption
        - redress and compensation

3) **Equitable, fair and just uses of data should be advanced: Place limits on certain data uses and safeguard equitable, fair and just outcomes**

Relying on "privacy self-management"—with the burden of responsibility placed solely on individuals alone to advance and protect their autonomy and self-determination—is not sufficient. Without one's knowledge or participation, classifying and predictive data analytics may still draw inferences about individuals, resulting in injurious privacy violations—even if those harms are not immediately apparent. Importantly, these covert practices may result in pernicious forms of profiling and discrimination, harmful not just to the individual, but to groups and communities, particularly those with already diminished life chances, and society at large. Certain data practices may also unfairly influence the behavior of online users, such as children.

Legislation should therefore address the impact of data practices and the distribution of harm by

a) placing limits on collecting, using and sharing sensitive personal information (such as data about ethnic or racial origin, political opinions/union membership, data concerning health, sex life or sexual orientation, genetic data, or biometric data) or data that reveals sensitive personal information, especially when using these data for profiling;
b) otherwise limiting the use of consumer scoring and other data practices, including in advertising, that have the effect of disproportionally and negatively affecting people's life chances, related to, for example, housing, employment, finance, education, health and healthcare;
c) placing limits on manipulative marketing practices;
d) requiring particular safeguards when processing data relating to children and teens, especially with regard to marketing and profiling.

4) **Privacy legislation should bring about real changes in corporate practices: Set limits and legal obligations for those managing data and require accountability**
Currently companies face very few limitations regarding their data practices. The presumption of "anything goes" has to end. Legislation should ensure that entities collecting, using, sharing data
    a) can only do so for specific and appropriate purposes defined in advance, and subject to rules established by law and informed by data subjects' freely given, specific, informed and unambiguous consent; for the execution of a contract, or as required by law; and without "pay-for-privacy provisions" or "take-it-or leave it" terms of service.
    b) notify users in a timely fashion of data transfers and data breaches, and make consumers whole after a privacy violation or data breach;
    c) cannot limit consumers' right to redress with arbitration clauses;
    d) are transparent and accountable, and adopt technical and organizational measures, including
        i. provide for transparency, especially algorithmic transparency,
        ii. conduct impact assessments for high-risk processing considering the impact on individuals, groups, communities and society at large,
        iii. implement *Privacy by Design and by Default,*
        iv. assign resources and staff, including a Data Protection Officer,
        v. implement appropriate oversight over third-party service providers/data processors,
        vi. conduct regular audits
    e) are only allowed to transfer data to other countries/international organizations with essentially equivalent data protections in place.

5) **Privacy protection should be consequential and aim to level the playing field: Give government at all levels significant and meaningful enforcement authority to protect privacy interests and give individuals legal remedies**
Without independent and flexible rulemaking data-protection authority, the Federal Trade Commission has been an ineffective agency for data protection. An agency with expertise and resources is needed to enforce company obligations. Ongoing research is required to anticipate and prepare for additionally warranted interventions to ensure a fair marketplace and a public sphere that strengthens our democratic institutions. Legislation should provide
    a) for a strong, dedicated privacy agency with adequate resources, rulemaking authority and the ability to sanction non-compliance with meaningful penalties;
    b) for independent authority for State Attorneys General;
    c) for statutory damages and a private right of action;
    d) for the federal agency to establish an office of technology impact assessment that would consider privacy, ethical, social, political, and economic impacts of high-risk data processing and other technologies; it would oversee and advise companies on their impact-assessment obligations.

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,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

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[5] (collection limitation, data

---

[1] *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.
[2] 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.
[3] 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.
[4] *Id.*
[5] 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.

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.

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

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

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

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

4. Legislation should provide redress for privacy violations

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

Signed,

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