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