THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Public Interest Comment[1] on

The National Telecommunications and Information Administration's Request for Comment

Developing the Administration's Approach to Consumer Privacy

Docket ID No. 180821780-8780-01
RIN: 0660-XC043

November 09, 2018

Daniel R. Pérez, Senior Policy Analyst[2]

The George Washington University Regulatory Studies Center

The George Washington University Regulatory Studies Center improves regulatory policy through research, education, and outreach. As part of its mission, the Center conducts careful and independent analyses to assess rulemaking proposals from the perspective of the public interest. This comment on the National Telecommunications and Information Administration's (NTIA) request for public comments on developing the administration's approach to consumer privacy does not represent the views of any particular affected party or special interest, but is designed to evaluate the effect of NTIA's proposal on overall consumer welfare.

Introduction

NTIA is requesting public comments on its proposed approach to guide federal policymaking related to consumer privacy. The agency's approach is divided in two parts: 1) a list of privacy outcomes that "any Federal actions on consumer-privacy policy" should aim to achieve, and 2) a list of high-level goals "setting the broad outline for the direction that Federal action should take."

[1] This comment reflects the views of the author, and does not represent an official position of the GW Regulatory Studies Center or the George Washington University. The Center's policy on research integrity is available at http://regulatorystudies.columbian.gwu.edu/policy-research-integrity.

[2] Daniel Pérez is Senior Policy Analyst at the George Washington University Regulatory Studies Center. He can be reached at danielperez@gwu.edu or (202) 994-2988.

The increased role of data collection and analysis in modern economies along with the growth of emerging technologies such as highly automated vehicles and unmanned aircraft systems bring privacy concerns to the forefront—particularly regarding the proper role of government intervention. NTIA's stated justification for the need to expand federal policymaking on consumer privacy protections is, at least in part, driven by international and domestic efforts to enact more stringent privacy and data protection regimes—such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018.[3] The agency notes that these "distinct visions for how to address privacy concerns [lead] to a nationally and globally fragmented regulatory landscape" with the potential to reduce economic growth and innovation in the data sharing economy.

It is, therefore, reasonable that the agency is taking steps to minimize the costs of a patchwork of disparate privacy regimes. Nonetheless, the agency's list of outcomes that "should be produced by *any* Federal actions on consumer privacy" is not an appropriate framework for regulation. The list implies that regulation to increase privacy protections in each category would—by design—generate better outcomes for the public. My own research on privacy controls identifies a broad base of evidence that consumers enjoy substantial benefits by gaining access to online content and other services in exchange for allowing use of their data; in contrast, there is little evidence that this exchange results in costly harms to consumer that outweigh these benefits (i.e., possibly presenting a compelling public need that might suggest the use of regulation).[4] Consequently, it is not accurate to presume that NTIA's list of outcomes will necessarily produce net beneficial results for the public.

This comment proposes the following recommendations for NTIA to consider:

1. **Privacy regulation should be based on evidence that regulation will actually advance privacy outcomes in ways that consumers value.** Evidence-based regulation (EBR)—successful implementation of evidence-enhancing strategies—is a more appropriate framework to guide regulatory decisions.
2. **The benefit of regulating consumer privacy should exceed the social cost—including costs consumers will bear as a result of regulation.**
3. **Further research should focus on generating useful empirical estimates of the benefits and costs of privacy controls.**

---

[3] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en; https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[4] Joseph J. Cordes & Daniel R. Pérez, "Measuring Costs and Benefits of Privacy Controls: Conceptual Issues and Empirical Estimates." Journal of Law, Economics and Policy. Vol 15, No. 1 (Fall 2018, forthcoming). Working paper available at: https://regulatorystudies.columbian.gwu.edu/measuring-costs-and-benefits-privacy-controls-conceptual-issues-and-empirical-estimates.

This comment references the following research which, per NTIA's Instructions for Commenters, I submit as attachments along with the comment:

- Marcus Peacock, Sofie E. Miller, and Daniel R. Pérez, "A Proposed Framework for Evidence-Based Regulation." The George Washington University Regulatory Studies Center. February 22, 2018.
- Joseph J. Cordes & Daniel R. Pérez, "Measuring Costs and Benefits of Privacy Controls: Conceptual Issues and Empirical Estimates." Journal of Law, Economics and Policy. Vol 15, No. 1 (Fall 2018, forthcoming).

Background on Interagency Policy Task Force—Privacy Initiative

Located within the Department of Commerce (DOC), NTIA is responsible for advising the president on telecommunications and information policy issues.[5] The agency's request for comment is part of its work as a member of the Internet Policy Task Force—an interagency task force DOC created to review policy issues including privacy, copyright, global free flow of information, and cybersecurity.[6] NTIA's proposed approach to guide federal consumer-privacy policy is the result of this interagency process led by the National Economic Council in coordination with the International Trade Administration and the National Institute of Standards and Technology.

NTIA Proposed Privacy Outcomes

The agency proposes several "principle-based approaches" to privacy, stating that it intends to avoid overly-prescriptive policies that "stymy innovating privacy solutions [while] not necessarily providing measurable privacy benefits." It is worth noting that NTIA's list of broadly-defined, normative privacy principles closely parallels several of the elements of the EU's GDPR regulation—albeit with less specificity or proposed stringency regarding penalties (i.e., fines for noncompliance).[7]

1. **Transparency**. Users should be provided the opportunity to give informed consent in such a way that they understand the manner in which entities are collecting, storing, and using their personally identifiable information (PII).
2. **Control**. Consumers should have some measure of control over the collection, storage, and use of their data.

[5] https://www.ntia.doc.gov/

[6] https://www.ntia.doc.gov/category/internet-policy-task-force

[7] https://eugdpr.org/the-regulation/

3. **Reasonable Minimization**. "Collection, storage, length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm."
4. **Security**. "Organizations…should employ security safeguards to secure these data [PII]. In short, users should have a reasonable expectation that their PII are protected from unauthorized access, destruction, etc.
5. **Access and Correction**. Users should have "reasonable [ability] to access personal data that they have provided, and to rectify, complete, amend, or delete this data."
6. **Risk Management**. Organizations should use risk-based approaches to reduce the risk of potential harm to consumers and increase user privacy.
7. **Accountability**. Entities should be accountable—both internally and to external audiences—while using approaches "that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes… [while taking] steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data."

NTIA Proposed Goals for Federal Action

The proposal lists eight goals intended to set a broad outline for the direction that it suggests the federal government take to increase consumer privacy.

1. **Harmonize the regulatory landscape**. NTIA states that "…there is a need to avoid duplicative…privacy-related obligations placed on organizations [by] the production of a patchwork of competing and contradictory baseline laws."
2. **Legal clarity while maintaining the flexibility to innovate**. "The ideal end-state would ensure that organizations have clear rules…while enabling flexibility that allows for novel business models and technologies…"
3. **Comprehensive application.** "Any action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities…not covered by sectoral laws."
4. **Employ a risk and outcome-based approach.** "Instead of creating a compliance model that creates cumbersome red tape…the approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes."
5. **Interoperability**. NTIA seeks "to reduce the friction placed on the data flows by developing a regulatory landscape that is consistent with…international norms and frameworks…"
6. **Incentivize privacy research**. "The U.S. government should encourage more research…into understanding user preferences, concerns, and difficulties… [to] inform the development of standards, frameworks, models, methodologies, tools, and products…"

7. **FTC enforcement**. "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."
8. **Scalability**. "[NTIA] 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."

Evidence-Based Regulation

Scholars and practitioners widely agree that the systematic application of evidence-based approaches is a necessary and valuable input in the creation of effective public policy.[8] Notably, the federal regulatory process is a distinct policy process that requires a tailored approach for successful implementation of evidence-enhancing strategies.[9] For example, the Administrative Procedure Act of 1946[10] compels agencies to justify most regulatory decisions based on the data, analyses, and other information collected and made part of a publicly available record.[11] Additionally, regulators should be able to demonstrate they are benefitting people's lives by creating policies that address a "compelling public need," as directed by Executive Order 12866.[12]

Regulation intended to increase consumer privacy benefits by simultaneously restricting the collection, storage, use, and/or sharing of data also imposes costs on society; a framework that produces evidence-based regulation requires assessment of the net effects of tradeoffs among expected benefits, costs, and other impacts of regulation.[13] NTIA's high-level goals should recognize that regulation is only an appropriate policy instrument for achieving a privacy outcome "upon a reasoned determination that the benefits of the intended regulation justify its costs."[14]

The agency repeatedly mentions its intent to "advance consumer privacy while protecting prosperity and innovation." Achieving this balance will require recognizing that it may not make sense for regulators to use NTIA's list of outcomes as a checklist (i.e., as a prerequisite) for designing effective privacy regulation. As the Office of Management and Budget notes in its guidance for conducting regulatory analysis, absent a clearly identified market failure, regulation

---

[8] The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking (September 2017). Available at: https://www.cep.gov/content/dam/cep/report/cep-final-report.pdf

[9] Peacock, Miller, and Pérez, "A Proposed Framework for Evidence-Based Regulation" The George Washington University Regulatory Studies Center. (February 2018). Available at: https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs1866/f/downloads/Peacock-Miller-Perez_Evidence-Based-Regulation.pdf

[10] Pub.L.No. 79-404, 60 Stat. 237.

[11] Ibid. p. 4.

[12] Executive Order 12866, "Regulatory Planning and Review," September 30, 1993.

[13] Peacock et al., above at 10.

[14] Executive Order 12866, "Regulatory Planning and Review," September 30, 1993.

can disrupt competition and lead to misallocation of resources—potentially leaving consumers worse off.[15]

In short, deciding that an outcome is worth achieving via regulation prior to assessing the evidence on the expected benefits and costs puts the proverbial cart before the horse (i.e., it is several steps along in the process of regulatory design).[16]

Evidence: Empirical Estimates of Privacy Benefits and Costs

Operationalizing the concept of privacy is complex, and thoughtful research designs to estimate the benefits and costs of privacy controls are most valid within the context of particular privacy issues.[17] In this regard, NTIA's list of privacy outcomes is a valuable approach since it attempts to operationalize privacy into discrete categories. However, as the agency notes, "they should [also] be read as a set of *inputs* for building better privacy protections."[18] Deciding what combination of inputs would likely generate net benefits via regulation to increase privacy protection requires empirical measures of benefits and costs.

Research attempting to generate measures of the benefits and costs of various privacy controls indicates that it is difficult to generate valid (and stable) estimates of consumers' willingness to pay (WTP) to protect their privacy.[19] In addition, these estimates are context-dependent (i.e., they are contingent on the way privacy is being operationalized and are highly sensitive to consumer characteristics such as gender) and also highly contingent on endowment effects (i.e., whether policies take away something consumers already have or grants them something they currently do not have).[20] Nonetheless, carefully specified research designs can generate useful "plug-in" values of both the social benefits and social costs of privacy regulation.[21]

---

[15] Office of Management and Budget, Circular A-4: Regulatory Analysis (September 17, 2003). Available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A4/a-4.pdf

[16] See: Peacock et al., above at 10, p. 6. See also: Adam Thierer, "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," George Mason Law Review, Vol. 20, No. 4 (Summer 2013).

[17] Cordes and Pérez, above at 4, p. 12.

[18] Emphasis added.

[19] See: Cordes and Pérez, above at 4, p. 13.

[20] Ibid. Regarding the endowment effect on estimates of privacy valuations, see: Acquisti, John, and Loewenstein, "What is Privacy Worth?" Journal of Legal Studies, Vol 42 (2013), pp. 249-74. Given that most people effectively pay nothing for digital services (they provide their private information in exchange for "free" use) Cass Sunstein recently refers to this as a "superendowment effect." See: Sunstein (2018) "How Much Would You Pay to Use Facebook? A Behavioral Perspective," Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3173687.

[21] Cordes and Pérez, above at 4, p. 14.

Substantial Benefits of the Digital Economy

Although the stated preference of U.S. consumers—generally speaking—is that they value their privacy highly,[22] their behavior in the market suggests that at a minimum, they receive a commensurate benefit from the use of social media, smartphone applications, and other digital content requiring them to exchange their PII for access. For example, a 2013 study found that a representative U.S. consumer was willing to pay between $1 and $4 to conceal various types of personal information (e.g., browser history, phone's unique identification number) from companies and third parties when downloading smartphone apps.[23] Notably, given that the typical app in the market is provided for free, the study estimated a lower-bound benefit to consumers from use of apps of approximately $17 billion—or around $5.00 per app.[24]

The fact that access and use of much of the digital economy is "free"—or, more appropriately stated: provided in exchange for user data which is then monetized in various ways by companies—is often considered problematic for generating valid estimates of consumers' willingness to pay for privacy (i.e., they usually pay nothing and exchange varying amounts of their PII). Nonetheless, researchers often find clever ways to design studies such that they provide more valid estimates. For instance, this might involve the use of deception to (albeit temporarily) fool participants into thinking they are making binding commitments to either pay or receive compensation in exchange for their choices.[25] A recent pilot experiment of this type estimated that Facebook users would have to be compensated about $60 per month to voluntary give up access to the social media platform.[26]

Evidence of Social Costs

Currently, a survey of the peer-reviewed literature on privacy generates no systematic evidence of social welfare losses incurred by consumers as a result of *most* uses of their data. The notable exception involves data misuse with the intent to cause economic harm (such as identity theft and other financial fraud). But this is an issue of data protection rather than data privacy.[27] For example,

---

[22] For example, a 2014 survey conducted by Pew found that "91% of Americans 'agree' or 'strongly agree' that people have lost control over how personal information is collected and used by all kinds of entities. Available at: http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[23] Savage and Waldman "The Value of Online Privacy" (2013) SSRN. Available at: https://ssrn.com/abstract=2341311

[24] Ibid. p. 3. The authors assumed that the typical app in the market is free, requires users to allow advertising, and requires the user to exchange their personal information including their location data and phone unique identification number.

[25] See Cordes and Pérez, above at note 4, p. 13.

[26] Sunstein, above at note 21.

[27] See, for instance: Brody, Mulig, and Kimball (2007), "Phishing, Pharming and Identity Theft" Academy of Accounting and Financial Studies Journal, Vol. 11, No. 3.

a recent study estimated financial losses incurred in the U.S. due to identity fraud in 2016 of $16 billion.[28] Even here, the full amount does not accrue as a social cost to consumers—who bear approximately only 10% of these losses.[29] This is partly a design of existing U.S. consumer protection laws.[30] The substantial losses incurred by credit card companies and other financial institutions suggests that they have powerful incentives to invest in data security.

Other scholars have suggested theoretical scenarios where regulation might be justified including preventing PII from being used for price discrimination[31] or ameliorating potential information asymmetries between consumers and firms.[32] Contrary to the presumption of information asymmetry, a recent empirical study of 1,600 randomly-selected Internet users in the U.S. found that 90% of respondents were generally familiar with Google's business practices concerning the use of consumer PII, 75% knew that Google collected their location data, and 88% knew that Google used their browser search data.[33]

The dearth of evidence of privacy-related harms to consumers suggests that regulators should be cautious of imposing restrictions that reduce the benefits that consumers seem to enjoy.

Recommendations

Before proceeding with privacy guidelines, NTIA should review the literature cited here and follow long-standing analytical practices[34] adopted to ensure federal policies do more good than harm. The first two recommendations below are absent from NTIA's outcomes or high-level goals and conform to current legal and administrative requirements on regulatory policymaking as well as best practices for producing evidence-based regulation.[35]

1. **Privacy regulation should be based on evidence that regulation will actually advance privacy outcomes in ways that consumers value**. NTIA should avoid assuming, *a priori*,

---

[28] Javelin Strategy and Research, "2017 Identity Fraud Study" Available at: https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

[29] Brody, Mulig, and Kimball, above at note 28.

[30] For instance, the Fair Credit Billing Act and the Electronic Fund Transfer Act offer various protections against fraud related to credit cards and use of other electronic fund transfers. See: https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards

[31] For instance, see: Borgesius and Poort "Online Price Discrimination and the EU Data Privacy Law" Journal of Consumer Policy, Vol. 40, No. 3 (September 2017).

[32] Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" Seattle University Law Review, Vol. 34, No. 1 (Fall 2010).

[33] Caleb Fuller, "Is the Market for Digital Privacy a Failure?" (2017) Available at: https://www.ftc.gov/system/files/documents/public_comments/2017/11/00019-141720.pdf

[34] Executive Order 12866, OMB Circular A-4 *Regulatory Analysis* (2003). Available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A4/a-4.pdf

[35] Peacock et al. above at note 10.

that more stringent privacy regulation would result in net benefits for consumers or that regulatory action should use the NTIA list of desired outcomes as a checklist.[36] Evidence indicates that consumers are consistently willing to trade their private data for what they perceive as the substantive benefits of using social media platforms, smartphone applications (apps), and various other digital goods—often provided for "free" (i.e., their cost is subsidized by company revenue generated by sales to advertisers or other uses of user data).[37] Scholars often refer to these people as "privacy pragmatists"—routinely willing to exchange their personal information for these benefits—and find little evidence that regulatory intervention to increase consumer privacy would be likely to generate net benefits for society.[38]

2. **The benefit of regulating consumer privacy should exceed the social cost—including costs consumers will bear as a result of regulation**. NTIA should explicitly consider costs, as well as benefits of any government action, as required by longstanding regulatory principles.
3. **Further research should focus on generating useful empirical estimates of the benefits and costs of privacy controls**.[39] NTIA lists incentivizing privacy research among its high-level goals and asks for public comment on the recommended focus and desired outcomes of exploring commercial data privacy-related issues. I suggest that further research should generate additional estimates of consumers' willingness to pay for privacy protections to increase the evidence of the social benefits and social costs of privacy regulation.[40]

---

[36] Alan McQuinn notes that "creating stronger privacy laws is simple. But creating stronger privacy laws that do not undermine the digital economy is much harder." See: Alan McQuinn,"Understanding Data Privacy" Real Clear Policy. Available at: https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html

[37] See: Sunstein (2018) above at note 21. Sunstein estimates a median monthly WTP for users in the U.S. to use Facebook of $1 while finding that the same user would need to be offered $59 to cease using Facebook for a month. Sunstein refers to this disparity as a "superendowment effect" that results from the intense opposition of people being asked to pay for a good that they had enjoyed for free.

[38] For instance, in a public interest comment submitted to the Federal Communications Commission on its proposal in 2016 to regulate the privacy practices of broadband Internet access service providers in an attempt to increase consumer privacy, Howard Beales noted that the agency's proposed regulatory intervention would likely result in a net loss to consumers and reduced innovation. See: Howard Beales, "Public Comment on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" The George Washington University Regulatory Studies Center, May 27, 2016. Available at: https://regulatorystudies.columbian.gwu.edu/public-comment-protecting-privacy-customers-broadband-and-other-telecommunications-services

[39] Cordes and Pérez, above at note 4.

[40] Id. p. 3.