January 14, 2019

Mr. David F. Alderman
Standards Coordination Office
National Institute of Standards and Technology
100 Bureau Drive, Stop 2100
Gaithersburg, MD 28099

COMMENTS OF PUBLIC KNOWLEDGE ON DEVELOPING A PRIVACY FRAMEWORK

Docket No. 181101997-8997-01

Public Knowledge thanks the National Institute of Standards and Technology ("NIST") for the opportunity to submit comments in response to its Request for Information ("RFI") in the above-captioned proceeding. Public Knowledge is a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works. These brief comments will provide a general response on how a useful and meaningful NIST Privacy Framework ("the Framework") might be developed.

Today's online surveillance economy is sustained by the extraordinarily privacy-invasive business practices of many companies operating in the internet ecosystem. Because internet users care deeply about their privacy,[1] these companies have powerful incentives to both obfuscate privacy-invasive practices and to define any recognized risks to consumer privacy as narrowly as possible. In view of these practices, the Framework must not be structured around a reductive definition of privacy risks that merely covers financial and physical harm. A voluntary framework based on such a myopic view of risks would not only fail to address the panoply of privacy harms that go beyond mere financial and physical harms, but it could also be used by industry to set an artificial and inadequate "floor" for privacy protections. This would be disruptive and counterproductive to efforts towards much-needed comprehensive federal privacy legislation, including the National Telecommunications and Information Administration's roughly parallel development of the Trump Administration's approach to consumer privacy.

[1] *See*, *e.g.*, Open-XChange, Consumer Openness Index 2016, 8 (2016), https://www.open-xchange.com/fileadmin/user_upload/open-xchange/document/report/open-xchange_coi_report_2016.pdf (84% of surveyed American internet users agreed that "everyone has a fundamental right to privacy.").

With this in mind, we strongly urge NIST to pursue the following courses of action when developing the Framework:

- Describe the impacts of privacy violations as harms
- Build the Framework around a comprehensive set of privacy risks that will address a broad and flexible definition of potential harms

While Public Knowledge believes that a rights-based approach is the proper framing for a national privacy regime,[2] to the extent that a voluntary, risk-based framework can be an effective tool for enterprise risk management, it is critical that it recognize the full scope of possible harms.

Describe the Impacts of Privacy Violations as Harms

NIST avoids using the word "harm" anywhere in its RFI, opting instead to describe, "the problems that individuals might experience as a result of the processing of their information, and the impact if they were to occur."[3] Such a framing is unsurprising in the context of an industry-driven framework, given that industry is typically only willing to recognize the existence of a small set of legally cognizable harms. Nevertheless, Public Knowledge emphasizes that consumer privacy harms are not merely "problems" or "issues" – they are actual harms that affect actual humans. Further, numerous privacy harms exist that extend beyond those that are currently legally cognizable. These harms are described in more detail in the following section. As a threshold matter, however, they are all harms and should be described as such both during the Framework's development and within the final Framework.

Build the Framework Around a Comprehensive Set of Privacy Risks that Will Address a Broad and Flexible Definition of Potential Harms

The privacy risk model set out in NISTIR 8062 provides a good starting point for defining privacy risks. First, it importantly defines privacy impacts in terms of harms – "Impact is the magnitude of cost or harm from the problematic data action." – and recognizes that privacy harms have an impact on an individual level.[4] As described above, privacy violations are harms and should be described as such in the final Framework. The 8062 risk model also acknowledges that assessing individual impact may also require considering "societal impacts on democratic institutions and quality of life."[5] NIST should build upon this foundation and develop the

---

[2] *See generally* Public Knowledge, Comments to the National Telecommunications and Information Administration, Docket No. 180821780-8780-01 (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/pk_ntia_comments_docket_no_180821780-8780-01_11-9-18.pdf. ("Public Knowledge NTIA Comments").
[3] Developing a Privacy Framework, 83 Fed. Reg. 56699, 56824, fn. 1 (Nov. 14, 2018).
[4] *See* Sean Brooks et al., *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems*, 22 (Jan. 2017), https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[5] *Id.*

Framework around a comprehensive set of risks, without limiting it to only the individualized injuries that are most readily cognizable under existing laws.

Financial loss and physical injury are a very small subset of the harms that can arise from the collection and misuse of data or from data breach, and they are among the hardest harms to prove. Even where financial loss arises from a data breach or the misuse of data – say, where a credit card number is stolen and fraudulent purchases are made – it is difficult to trace that stolen credit card to one particular data breach. And, where it is possible to trace back to the particular data breach, banks often reimburse customers for fraudulent purchases, obviating any actual direct financial loss.[6]

In fact, under current law, redress for the most pernicious harms associated with data breach and misuse of data may be uncertain at best. For example, a data breach may expose information that could be embarrassing or cause reputational harm, undermining one's employment or social prospects. Data that falls into the wrong hands could re-endanger a domestic violence victim. Harms may also come in the form of Cambridge Analytica-style "psychographics," misinformation, or distortions of the public record that undermine public trust in U.S. democratic institutions and put our national security at risk.[7] Irresponsible data use can exacerbate informational disparities, enable unfair price discrimination, limit awareness of opportunities,[8] and contribute to employment, housing, health care, and other forms of discrimination.[9] And the risks associated with data use and abuse will likely evolve as technology changes. This inherent complexity and unpredictability makes it even more crucial that NIST not adopt a restrictive view of harms.

The Framework should define risks with the goal of minimizing this broad array of potential harms. While assessing the impact cost associated with problematic data action is a challenge, the proxies outlined in NISTIR 8062 to help account for individual impact – i.e., compliance, mission failure, reputational, and internal culture costs – can also be useful in the context of an enterprise risk assessment framework.

---

[6] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases,* WALL STREET J. (June 26, 2016), https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.

[7] *See* Sen. Ron Wyden, *Facebook can't be trusted to protect users' data on its own. It's time for Congress to step in*, NBC NEWS (Dec. 20, 2018, 1:50 PM EST), https://www.nbcnews.com/think/opinion/facebook-can-t-be-trusted-protect-users-data-its-own-ncna950386.

[8] *See* Upturn, Leveling the Platform: Real Transparency for Paid Messages on Facebook (May, 2018).

[9] *See, e.g.*, Julia Angwin, Ariana Tobin, and Madeline Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA (Nov. 21, 2017); Natasha Singer, *Just Don't Call It Privacy*, NY Times (Sept. 23, 2018), https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.

Use of Personal Information for Cybersecurity Operations

Some personal information that can directly or indirectly reveal intimate details about one's life, such as IP addresses, may also be valuable or necessary for cybersecurity operations. Any uses of personal information for such cybersecurity purposes, regardless of its "sensitivity"[10] must nevertheless be consistent with the relevant practices of the ISAO Standards Organization, which Public Knowledge helped to develop.[11] These practices call for organizations to, "disclose, retain, and use information for a cybersecurity purpose *only* for cybersecurity purposes, as defined by CISA."[12]

Responding to #17: "Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks."

Privacy and cybersecurity are two sides of the same coin. So, at a minimum, the Privacy Framework should be compatible with the Cybersecurity Framework ("CSF"). One place to start could be to identify privacy protective actions within the each of the CSF's five top-level elements of identify, protect, detect, respond, and recover. Given the success of the CSF, it would be useful to identify an analogous set of top-level elements for the Framework. For example, the privacy elements could be: identify, inform, steward, respond, redress. Whatever form the final elements take, they should incorporate the critical privacy principles of control, choice, and context.

Respectfully Submitted,

Dylan Gilbert

[10] Public Knowledge believes that distinguishing between data or categorizing data based on levels of "sensitivity" is no longer necessary and should not be done. Instead, all data should be considered "sensitive" data. *See* Public Knowledge NTIA Comments at 3.
[11] *See* ISAO Standards Organization, ISAO SP 4000: Protecting User Privacy In Cybersecurity Information Sharing (July 26, 2017), https://www.isao.org/wp-content/uploads/2017/07/ISAO-SP-4000-Protecting-Consumer-Privacy-in-Cybersecurity-Information-Sharing-v1-0.pdf.
[12] *Id.* at 1 (emphasis added).