From: Jennifer Huddleston <Jhuddleston@mercatus.gmu.edu>
Sent: Thursday, October 24, 2019 10:51 AM
To: privacyframework <privacyframework@nist.gov>
Cc: Anne Hobson <Ahobson@mercatus.gmu.edu>; aparson6 <aparson6@masonlive.gmu.edu>
Subject: Submission of Comments

Attached please find comments regarding the proposed draft of the NIST Privacy Framework on behalf of myself and my Mercatus Center at George Mason University colleagues Anne Hobson and Anna Parsons.

Sincerley,

Jennifer Huddleston
Research Fellow, The Fourth Branch, Project on Innovation and Governance
Mercatus Center at George Mason University

MERCATUS CENTER
George Mason University

PUBLIC
INTEREST
COMMENT

MITIGATING PRIVACY RISKS WHILE ENABLING EMERGING TECHNOLOGIES

JENNIFER HUDDLESTON
Research Fellow, Fourth Branch Project, Mercatus Center at George Mason University

ANNE HOBSON
Program Manager, Academic & Student Programs, Mercatus Center at George Mason University

ANNA PARSONS
MA Fellow, Mercatus Center at George Mason University

Agency: National Institute of Standards and Technology
Comment Period Opens: September 9, 2019
Comment Period Closes: October 24, 2019
Comment Submitted: October 24, 2019
Docket No. 2019-19315

We appreciate the opportunity to provide comments on the preliminary draft *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (hereafter the Privacy Framework or the Framework) of the National Institute of Standards and Technology (NIST).[1] The Mercatus Center at George Mason University is dedicated to bridging the gap between academic ideas and real-world problems and to advancing knowledge about the effects of regulation on society. This comment does not represent the views of any particular party or special interest group but is designed to assist NIST in creating a policy environment that will facilitate increased innovation, competition, and access to technology to the benefit of the public.

We applaud NIST's efforts to empower enterprises to mitigate risk while also recognizing the potential impact of standards on emerging technologies. The request for comment recognizes that the digital space is a "complex ecosystem" with multiple stakeholders.[2] The Framework identifies stakeholders within the data processing ecosystem including manufacturers, government service providers, individuals, commercial service providers, developers, businesses, and suppliers.[3] The complexity of this ecosystem requires that the Privacy Framework function as one

[1] National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, September 6, 2019.
[2] National Institute of Standards and Technology, *NIST Privacy Framework*, 3.
[3] National Institute of Standards and Technology, 16.

For more information, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor, Arlington, VA 22201

part of a wider set of solutions and resources developed by stakeholders to mitigate risk. Toward this end, this comment addresses two of NIST's requests for review:

1. Whether the preliminary draft adequately defines the relationship between privacy and cybersecurity risk.
2. Whether the draft enables organizations to adapt to privacy risks arising from emerging technologies such as the internet of things (IoT) and artificial intelligence (AI).

In the sections that follow, we first suggest how the Framework can empower and educate individuals and civil society to mitigate privacy risk. We then propose resources worth including in the Framework's proposed resource repository and recommend using the terminology of resilience in specifying the Framework's goals. We highlight the importance of clarifications for the Framework's delineation between privacy and cybersecurity risk, and we caution that guidance on AI and the IoT should focus on existing incidents of harm rather than hypothetical risks. Finally, we recommend that the Framework include guidance on risks associated with government access to data.

THE FRAMEWORK'S ROLE IN EMPOWERING INDIVIDUALS AND CIVIL SOCIETY TO MITIGATE PRIVACY RISK

The proposed framework properly identifies enterprise risk management as one piece of a larger set of security and privacy efforts. By focusing primarily on the role of enterprises in risk management, NIST's approach has the potential to diminish the role individuals and civil society have in protecting data. A majority of data breaches and incidents result from human error and are thus unintentional or inadvertent.[4] Processes involving staff or users deserve further scrutiny throughout the five privacy framework functions; specifically, the framework should further emphasize privacy awareness and training, communication of privacy policies internally and externally, and access control regarding data.

Education empowers individuals to adopt good cybersecurity practices and engage in appropriate steps following a data breach.[5] In this regard, NIST should take seriously the Privacy Framework's role as an educational document for organizations. Aggregating resources and clarifying the responsibilities of organizations will better help these organizations avoid noncompliance with existing or forthcoming legislation. In addition to NIST's own resources, the following resources for the proposed repository of privacy resources are worth highlighting:

1. The Federal Trade Commission (FTC), in partnership with other federal agencies, has created OnGuardOnline, a website that offers privacy tips for individuals and businesses.[6]
2. The Future of Privacy Forum hosts a central repository of privacy resources regarding best practices for organizations.[7]

---

[4] Mahmood Sher-Jan, "Data Indicates Human Error Prevailing Cause of Breaches, Incidents," *Privacy Advisor*, June 26, 2018.
[5] Jennifer Huddleston, "The Importance of Avoiding Unintended Consequences When Defining Harm for Data Security and Data Privacy" (Testimony before House Committee on Oversight and Reform, Subcommittee on Economic and Consumer Policy, Mercatus Center at George Mason University, Arlington, VA, March 26, 2019).
[6] Federal Trade Commission, "OnGuardOnline," accessed October 10, 2019, www.consumer.ftc.gov/features/feature-0038-onguardonline.
[7] Future of Privacy Forum, "Best Practices," accessed October 10, 2019, https://fpf.org/best-practices/.

3. The Council of Better Business Bureaus has a set of data privacy guidelines for small businesses.[8]
4. TeachPrivacy is an educational platform for improving security and privacy awareness among employees.[9]
5. The Electronic Frontier Foundation offers tools to help individuals protect themselves online.[10]
6. The International Association of Privacy Professionals collects resources on organizational privacy policies, crafting a privacy notice, and existing privacy regulations.[11]

Furthermore, developments in liability standards and the role of tort law in privacy cases are worth understanding when considering the overall regulatory environment in which data privacy decisions are made.[12] NIST's privacy framework is one piece of an existing web of privacy resources and solutions that help organizations self-regulate and improve baseline privacy through suggested best practices. Given that civil society—including professional organizations, trade associations, research centers, and advocacy groups—supplies privacy resources, NIST should include civil society as a distinct party in the data processing ecosystem in section 3.5 of the Framework. The Framework recognizes that "deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions."[13] The proposed repository of privacy resources ensures that multiple solutions are available to enterprises.

THE FRAMEWORK'S ROLE IN FOSTERING A RESILIENT DATA PROCESSING ECOSYSTEM

NIST's Privacy Framework notes correctly that data actions can have unintended consequences for user privacy.[14] Requirements and recommendations intended to mitigate risk can also result in unintended consequences. For example, requirements can foster a false sense of security against privacy risk because organizations feel that they have "checked all the boxes." This belief can compromise an organization's preparedness to deal with emerging or evolving privacy risk.[15]

Regulatory frameworks can favor the most restrictive privacy preferences rather than supporting a wide range of individual preferences and potential improvements to security and privacy that may not yet be anticipated.[16] In this regard, we commend NIST for viewing risk mitigation as a task that is ongoing and evolving. In short, privacy practices must be continuously reevaluated, and resilience to risk must be achieved over and over again.[17] The framework acknowledges the importance of constant vigilance, organizational learning, and risk reassessment in the data processing ecosystem. NIST advances its framework with the following vision:

---

[8] Better Business Bureau, "Data Privacy for Small Businesses," accessed October 10, 2019, https://www.bbb.org/council/for-businesses/toolkits/data-privacy-for-small-businesses/.
[9] TeachPrivacy, TeachPrivacy home page, accessed October 10, 2019, https://teachprivacy.com/.
[10] Surveillance Self-Defense, Surveillance Self-Defense home page, accessed October 10, 2019, https://ssd.eff.org/en.
[11] International Association of Privacy Professionals, "ResourcesCenter," October 10, 2019, https://iapp.org/resources/.
[12] Privacilla, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, July 2002.
[13] National Institute of Standards and Technology, *NIST Privacy Framework*, 4.
[14] National Institute of Standards and Technology, 6.
[15] Anne Hobson, "Should the Government Require Companies to Meet Cybersecurity Standards for Critical Infrastructure?," *Wall Street Journal*, November 12, 2018.
[16] Alec Stapp, "Against Privacy Fundamentalism in the United States," *Niskanen Center*, September 12, 2019.
[17] Anne Hobson, "The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem" (Policy Paper No. 2019.004, Center for Growth and Opportunity at Utah State University, Logan, UT, July 2019), 16.

> The five Functions, defined below, are not intended to form a serial path or lead to a static desired end state. Rather, the [five] Functions should be performed concurrently and continuously to form or enhance an operational culture that addresses the dynamic nature of privacy risk.[18]

While the Framework accurately acknowledges the governance challenge in a dynamic and rapidly evolving ecosystem,[19] it occasionally undermines this stated vision. For example, the Framework aims to help organizations in "future-proofing products and services . . . in a changing technological and policy environment."[20] Future-proofing is an unachievable goal for a dynamic ecosystem because the future is unknowable and constantly changing. What's more, looking to future-proof using only existing technologies might actually prevent the emergence of new, innovative solutions that would better improve security and privacy. Instead, it is better to aim at fostering resilient products and services and encourage innovative solutions that can adapt to new threats. Resilience is a process of building the capacity to adapt to emerging threats.[21] There is a tension between mitigating risk in its entirety and achieving resilience to breaches and security threats. Exposure to risk is both inevitable and critical for allowing individuals inside and outside organizations to learn how to manage and adapt to privacy risk.[22] Rather than focus on "future-proofing," we encourage NIST to specify resilience to privacy risk as an end goal in the executive summary and introduction of the Privacy Framework.[23]

CLARIFYING PRIVACY AND CYBERSECURITY RISK

The Privacy Framework can benefit from further clarification on the distinction between cybersecurity and privacy risk management. Defining the boundaries between privacy and cybersecurity risk is challenging because of the subjective nature of privacy concerns.[24] Understanding risk requires identifying and defining privacy harm, as well as differentiating that harm from cybersecurity harm. Section 1.2.1 of the Privacy Framework has clarified this distinction for cybersecurity harm well, but its definition of privacy risks remains overly broad by not clearly distinguishing the risks or lack of risks associated with different types of personal information.

NIST's categorization of privacy risk could use further clarification. For example, personally identifiable information is defined as data that can be used to distinguish one person from another, such as social security numbers or biometric identifiers, the exposure of which poses greater risks to users than other types of data. An organization or bad actor knowing one's credit card information or address is riskier than knowing one's ice cream flavor preference. It is important to be specific about categories of data so organizations can identify the riskiest data actions for

---

[18] National Institute of Standards and Technology, *NIST Privacy Framework*, 9.
[19] Governance is defined as a process of interaction among decision makers that leads to informal or formal rules that constrain behavior. While government is recognized as providing formal governance, any organization or individual involved in the process of forming rules is producing, and often coproducing, governance. Hobson, "The Resilience Approach."
[20] National Institute of Standards and Technology, *NIST Privacy Framework*, 3.
[21] Hobson, "The Resilience Approach," 6.
[22] Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2014).
[23] Adam Thierer, Jennifer Huddleston, and Anne Hobson, "The Internet of Things and Consumer Product Hazards" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, June 14, 2018).
[24] Adam Theirer, "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law & Public Policy* 36, no. 2 (2013): 409–55.

scrutiny under the Framework. Without such distinctions, treating all information associated with an individual as having the same level of privacy risk can both deter future innovation as well as prevent already beneficial uses and can result in an overly expansive impact that fails to actually address privacy concerns.[25]

When setting standards for privacy and security, the focus should remain on preventing and mitigating clearly definable harms. This approach provides both consumers and providers with certainty regarding forbidden behaviors while still allowing innovative approaches to continue to flourish.[26] A harm-based approach that clearly defines the risks and actions that lead to such harms will best minimize the effect on innovation by presuming new uses allowable unless previously forbidden. The Framework must also take into account the strong likelihood that citizens, as in the past, will adjust their privacy expectations in response to ongoing marketplace and technological change. Not everyone shares the same sensitivities or values, and therefore defining privacy harm will continue to be a challenge.[27] While the Framework takes positive initial steps in defining harms associated with cybersecurity risks, we suggest that further clarification is necessary, particularly with regard to existing privacy-associated harms and categories of data.

ENABLING EMERGING TECHNOLOGIES THROUGH AN ADAPTIVE APPROACH TO CYBERSECURITY AND PRIVACY RISKS

We commend NIST for considering how the Framework will address privacy risk associated with emerging technologies such as the IoT and AI. It is important that the Framework not be so overly prescriptive and precautionary as to prevent innovations that could come from such technologies.[28] When faced with the rapid changes associated with technological advancement, the use of soft law can facilitate a governance approach that is able to evolve with and enable innovation better than traditional policy tools.[29] Soft law includes rules that are not strictly binding, such as best practices and voluntary frameworks (e.g., the Privacy Framework and the Cybersecurity Framework).

When determining what resources and practices are necessary regarding privacy and security for new technologies, the Framework should focus on responding to known risks. This approach will minimize unintended consequences and maximize the potential benefits of innovation while providing appropriate redress for those harmed and levying penalties for actors who break or evade the law.[30] Future recommendations for adapting to risks associated with the IoT and AI should focus on proven incidents of privacy risk and harm rather than hypothetical worst-case scenarios associated with these emerging technologies.

---

[25] Jennifer Huddleston, "Four Questions to Consider When Debating Potential Data Privacy Policy," *The Bridge*, April 25, 2019.
[26] Christopher Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, October 27, 2017).
[27] Adam Thierer, "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," *George Mason Law Review* 20, no. 4 (2013): 1055–1105.
[28] Ryan Hagemann, Jennifer Huddleston, and Adam Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future," *Colorado Technology Law Journal* 17, no. 1 (2019): 37–130.
[29] Hagemann, Huddleston, and Thierer, "Soft Law for Hard Problems."
[30] Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases"; Jennifer Huddleston, "The Importance of Balancing Privacy with Innovation, Consumer Benefits, and Other Rights in the FTC's Approach to Consumer Data Privacy" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, May 30, 2019); Jennifer Huddleston, "The Importance of Avoiding Unintended Consequences."

ARTIFICIAL INTELLIGENCE

AI is increasingly used both to extract data and to defend against data extraction. The dual nature of this emerging technology complicates a comprehensive approach to mitigating cybersecurity or privacy risk in the data processing ecosystem. What's more, certain AI applications such as machine learning rely on large datasets for training. Many of the concerns about such datasets can be addressed by existing tools regarding breach, security, and consent.[31] Education, social pressure, societal norms, voluntary self-regulation, and targeted ex post enforcement through common law or FTC action already work to constrain bad use cases. Beyond agency action, the courts and common law are also often able to address various issues through product liability or other appropriate claims on an ex post basis.[32] These ex post adaptive tools are better able to address concerns about potential misuse and abuse of data actions than are regulatory requirements or prescriptive frameworks.

As our Mercatus colleague Adam Thierer has written,

> In particular, policymakers should prioritize developing an appropriate understanding of the varied sector of artificial intelligence technologies from the outset and developing an appreciation for limitations of our ability to forecast either future AI technological trends or crises that may ultimately fail to materialize.[33]

The framework should focus on those AI applications that have been linked to specific harms rather than applications perceived to have high privacy risks. For example, AI-driven predictive policing and criminal sentencing software result in known civil-liberties concerns. In this case, more accountability mechanisms may be appropriate.[34] Basing policy on evidence, rather than fear of worst-case uses of AI, can foster the right balance between mitigating privacy risk and promoting innovation.

THE INTERNET OF THINGS

The IoT is a network of connected devices that send and receive data.[35] It includes devices from smartphones and computers to autonomous vehicles and mesh networks. As the amount and type of connected devices have grown, so have privacy and cybersecurity concerns. Yet there are several benefits of such technologies for consumers, including the ability to help disabled and aging populations have greater independence.[36] Rather than focus exclusively on the potential problems from data security and privacy, the benefits of IoT devices should also be acknowledged in the Framework.[37] When addressing harm, guidance should be narrowly tailored to address the exact harm and the specific technology involved rather than using a broad approach that could have unintended consequences for both current and future connected devices and data usage.

---

[31] Adam Thierer, "Artificial Intelligence and Public Policy" (Mercatus Research, Mercatus Center at George Mason University, Arlington, VA, 2017).
[32] Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases."
[33] Thierer, "Artificial Intelligence and Public Policy," 5.
[34] Thierer, 37.
[35] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World" (R Street Policy Study No. 86, R Street Institute, Washington, DC, February 2017).
[36] Christian Vogler, "IoT Called a 'Wonderful Thing' for People with Disabilities," *MeriTalk*, November 7, 2016; Charles Consel and Jeffrey A. Kaye, "Aging with the Internet of Things," *The Bridge* 49, no. 1 (2019): 6–12.
[37] Adam Thierer, "Converting Permissionless Innovation into Public Policy: 3 Reforms," *Plain Text*, December 6, 2017.

The governance challenge facing the IoT data ecosystem is unique because of the ecosystem's dynamism, complexity, and decentralized and distributed nature. A narrow prescription for IoT privacy practices could discourage flexibility and offset the ecosystem's ability to manage risk.[38] IoT devices are increasingly intertwined with AI capabilities. For example, smart routers use a combination of AI and cloud services to recognize, monitor, and identify threats from malware and botnets to household IoT devices. As with AI, it is important that policy suggestions related to the IoT be responsive to known challenges, rather than anticipatory, and focus on known harms and risks rather than applying to a general-purpose technology.[39]

While it is useful for NIST to think about the impact of AI and the IoT, many of the concerns are tied to the same underlying cybersecurity and privacy risks associated with existing internet technologies. NIST's guidance should also recognize that these emerging technologies have the potential to prevent certain risks through an improved ability to identify security weaknesses as well as opportunities to decentralize information or improve authentication for access.

DISTINGUISHING GOVERNMENT REQUESTS AND USE OF DATA FROM PRIVATE INDUSTRY DATA USAGE

Currently, the Privacy Framework only focuses on data actions associated with enterprise data collection and usage. The Framework should be careful to distinguish government use of data from its use by private industry or civil society.

Law enforcement requests for access and government-mandated access to user data complicate the task of mitigating privacy risk. Government requests for user data have increased steadily as more activity has moved online.[40] Privacy risks associated with foreign or domestic government access to user data should be included in each of the five Privacy Framework functions, starting with "Identify-P." Documents referring to requirements under Section 702 of the FISA Amendments Act of 2008 and Mutual Legal Assistance Treaty requirements for cross-border data flows should be included in the proposed resource repository.[41]

Notably, guardrails can be established that limit potential abuse of technology by the government but still allow beneficial uses by both the public and private sectors. For example, placing harms-based restrictions on specific government uses rather than on a technology more generally can help reduce the potential abuses.[42]

With the growth and deployment of data through various connected devices from smartphones to scooters, conversations about government access to this data from both its own collection and private industry are increasingly likely to be part of the policy conversation around emerging technologies.[43] Such data can be useful to government entities for the provision of services such as access to public transportation, but they also have the potential for abuse that

---

[38] Hobson, "The Resilience Approach," 16.
[39] Adam Thierer, "The Connected World: Examining the Internet of Things" (Testimony before the Senate Committee on Commerce, Science and Transportation, Mercatus Center at George Mason University, Arlington, VA, September 15, 2019).
[40] Arthur Rizer and Anne Hobson, "Cross-Border Data Requests: Evaluating Reforms to Improve Law Enforcement Access" (R Street Policy Study No. 120, R Street Institute, Washington, DC, November 2017).
[41] Rizer and Hobson, "Cross-Border Data Requests."
[42] Matthew Feeney, "Should Police Facial Recognition Be Banned?," *Cato at Liberty*, May 13, 2019; Adam Thierer, "The Great Facial Recognition Technopanic of 2019," *The Bridge*, May 17, 2019 (discussing similar balancing in government use of facial recognition technologies).
[43] Jennifer Huddleston and Trace Mitchell, "Should Shared Mobility Services Share Your Data?," *The Bridge*, September 4, 2019.

could limit individual freedom. For example, government's ability to identify and actively track its citizens can result in false positives in terms of detainments and arrests. It is important for the Framework to acknowledge these risks through access to appropriate policy resources as well as distinguish government data actions from consumer and private actions.

CONCLUSION

We agree with NIST's vision to provide a common language for stakeholders and improve privacy through enterprise risk management. The role of government in addressing cybersecurity and privacy risk is to foster a policy environment such that a wide set of solutions can evolve. By cultivating a resource repository, promoting the adoption of guidelines and best practices, and encouraging enterprises to dynamically respond to harm, the NIST Privacy Framework promises to do just that.

We encourage NIST to emphasize resilience to privacy risk as an aim of the Framework, to limit the guidance and restrictions on data related to AI and the IoT to existing known privacy risks, and to consider potential civil-liberty and privacy risks related to government access to data. Still, we encourage a framework that is rooted in harm rather than a more amorphous standard that could deter future innovation and the development of better tools to allow individuals and enterprises to manage their privacy and security risks.