From: Alexandra McLeod <AMcleod@actonline.org>
Sent: Thursday, October 24, 2019 3:56 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Brian Scarpelli <BScarpelli@actonline.org>
Subject: NIST Privacy Framework: Preliminary Draft Comments - ACT | The App Association
Importance: High

Dear NIST Staff,

Please find attached ACT | The App Association's ("The App Association") comments regarding the Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. The App Association appreciated the opportunity to provide feedback on this preliminary draft and we look forward to working with NIST in the future on this issue.

If you have any further inquiries please contact Brian Scarpelli or Alexandra McLeod (contact information listed below).

All the best.

Alex and Brian

Brian Scarpelli
Senior Global Policy Counsel
+1 517-507-1446 | bscarpelli@actonline.org
ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

Alexandra McLeod
Associate Policy Counsel
+1 (209)-914-8912 (m) | amcleod@actonline.org
ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

October 24, 2019

ATTN: Katie MacFarland
U.S. Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive
MS 2000
Gaithersburg, Maryland 20899

RE: *Comment of ACT | The App Association to the National Institute of Standards and Technology on the* Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management *[Docket No. 2019-19315; 84 FR 47255]*

ACT | The App Association ("The App Association") submits these comments in response to the U.S. National Institute of Standards and Technology's (NIST) request for comments (RFC) on its *Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* ("Preliminary Draft").[1] NIST's Preliminary Draft is timely and important to the national dialogue on privacy risk management, and the App Association appreciates the opportunity to provide commentary on it. The App Association supports public-private partnership initiatives and strategies, including the development of the NIST Privacy Framework, to advance policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services.

[1] *The Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, 84 Fed. Reg. 47255 (September 9, 2019).

The App Association represents more than 5,000 small business mobile software and connected device companies that have created a $1.7 trillion industry supporting 5.9 million jobs in the United States. App Association members lead America's next industrial revolution, transforming traditional industry sectors and government functions—from healthcare and public safety to manufacturing and municipal government—into dynamic, data-driven, and mobile enterprises. Today, the "tech industry" no longer exists as a separate, unique vertical.[2] Rather, it has expanded and taken root as part of other industries, and in the process, it has been democratized into a startup economy that thrives across the nation—mostly outside of Silicon Valley. As cars begin to drive themselves and physicians adopt clinical decision tools that utilize artificial/augmented intelligence (AI), the United States is fast evolving into a "tech economy."[3]

The App Association serves as a leading resource for thought leadership and education for the American small business technology developer community in the privacy space. We regularly work to keep our members up-to-speed on the latest policy and legal developments and to translate those into practical and useable guidance to ease the burden of compliance.[4] We are committed to promoting proactive approaches to ensuring end-user privacy and note our endorsement of privacy-by-design approaches.[5]

As regulators from across key markets abroad continue to immediately utilize regulatory approaches for the digital economy which are often heavy-handed, the United States has remained the greatest market in the world for building a startup due to its evidence-based and light-touch approach to regulating new industries. Across the world, other governments struggle to incent and sustain the digital economy growth seen only in this country because companies elsewhere often face greater barriers to bringing novel products and services to market—slowing technological innovations to the pace of government approval.

The American approach to privacy is a work in progress, and the App Association agrees that the time for changes to the U.S. approach to privacy regulation has arrived. Federal sector-specific regulation of privacy, along with a patchwork of state-level laws and regulations, presents a very challenging scenario for a small business innovator. The App Association is supportive of a new federal privacy framework that will clarify the obligations of our members and generally urges that the U.S. approach to privacy provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation. NIST's Privacy Framework can and should inform the continuing discussions surrounding the federal legislative process and other policymaker approaches to privacy.

---

[2] Reed, Morgan, *There is no "tech industry,"* ACT | The App Association blog, Reed, Morgan, *There is no "tech industry,"* ACT | The App Association blog (Oct. 24, 2017). (Oct. 24, 2017).

[3] *Id*.

[4] *See*, *e.g.*, ACT | The App Association, *General Data Protection Regulation Guide* (May 2018), *available at* https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf.

[5] RFC at 48602.

The App Association supports public-private partnership initiatives and strategies, including NIST's development of the Privacy Framework, to advance policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services. We continue to work with our members to advance improved privacy approaches from the earliest stages and throughout a product's lifecycle. Small businesses represent 99.9 percent of all U.S. firms[6] and must play a more significant role in the development of privacy management strategies. NIST must remain mindful of the fact that large companies often dedicate large budgets to creating and maintaining privacy control processes and can hire staff and consultants to mitigate privacy risks, while small enterprises often cannot afford these large expenses. For many of our members, the role of chief privacy officer may be one of five (or more) hats worn by a single employee. The essential role of American small businesses, along with the unique resource constraints they face, make policymaker efforts like the NIST Privacy Framework even more important.

As noted in our prior comments, the App Association continues to urge NIST to ensure, consistent with its approach to the NIST Cybersecurity Framework, that its Privacy Framework provides a scalable, flexible, voluntary toolbox that any organization can use. We would like to reiterate that our small and medium enterprise (SME) members often struggle with the detail and complexity of the Cybersecurity Framework, making it difficult to fully leverage the Cybersecurity Framework. Small businesses rarely have the precious time and resources needed to review and implement dense documents, particularly those that recommend consultation with large suites of risk management standards or require expensive certifications.

The App Association is encouraged by the development of the Privacy Framework as an operational framework to advance privacy engineering but urges NIST to take additional steps to make its Privacy Framework as understandable and actionable as possible for small businesses that often face extreme resource and time constraints. We urge NIST to take the additional step and further define privacy engineering fundamentals in a small business-focused Privacy Framework (much like what NIST developed for the NIST Cybersecurity Framework[7]). In addition, the Federal Trade Commission (FTC) has developed best practices in the form of its Start with Security guide for SMEs, which draws from the NIST Framework,[8] and we encouraged NIST to work with the FTC in a similar campaign to assist small businesses in addressing privacy.

These small business-targeted efforts by NIST, the FTC, and other agencies are a great start, but we have much work to do. Bottom lines often drive business decisions; therefore, we suggest that future education efforts in partnership with key agencies including the Small Business Administration help to make the business case (i.e., it provides a return on investment) for using the future Privacy Framework. The App Association is committed to advancing privacy

[6] https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/24153946/Frequently-Asked-Questions-Small-Business-2019-1.pdf.

[7] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[8] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

engineering throughout our community through direct member education and public-private partnerships like the Information Technology Sector Coordinating Council, and other means. We are committed to working closely with NIST and other public and private stakeholders throughout the development and implementation of this Framework allowing for more small business-focused privacy risk management practices that support the growth of the digital economy.

Further, in response to NIST's Preliminary Draft, the App Association offers the following input:

- The App Association supports the proposed Function-Category-Subcategory Core structure being employed by the Privacy Framework. We approve of NIST's Preliminary Draft providing a flexible privacy framework that is customizable to an individual organization's needs. Specifically, the Preliminary Draft emphasizes that NIST does not require a "prescribed" privacy profile template, but instead allows for a malleable template to manage each organization's specific privacy needs.

- The App Association supports NIST's sector-agnostic approach to the Privacy Framework, as well as the Preliminary Draft's references to having a technology-neutral approach when implementing the Privacy Framework.

- Technical protection mechanisms (TPMs), including the use of end-to-end encryption, are essential elements in responsible privacy engineering, yet the Preliminary Draft does not adequately discuss such tools, nor does it endorse their use in privacy engineering. The App Association believes this is an oversight and strongly encourages NIST to ensure that its Privacy Framework (1) define key TPMs and (2) describe their vital role in sound privacy engineering practices.

The App Association supports NIST's development of a Privacy Framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information. We look forward to our continued work with NIST and other stakeholders on developing an environment that protects privacy, prosperity, and American economic leadership.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Alexandra McLeod
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 500)
Washington, DC 20005