January 14, 2019

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

RE: *Comments of ACT | The App Association to the National Institute of Standards and Technology on* Developing a Privacy Framework *[Docket No. 181101997-8997-01; 83 FR 56824]*

ACT | The App Association submits these comments in response to the U.S. National Institute of Standards and Technology (NIST) request for information (RFI) on developing a 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.[1] This RFI, and NTIA's work in the privacy space, is timely, and the App Association appreciates the opportunity to provide commentary in response to the questions presented. We support 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] *Developing a Privacy Framework*, 83 Fed. Reg. 56824 (Nov. 14, 2018).

The App Association represents more than 5,000 small to mid-sized mobile software and connected device companies in a $950 billion industry that supports 4.7 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 sector" no longer exists as a separate, unique vertical. 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 intelligence (AI), the United States is fast evolving into a "tech economy."[2] Moreover, companies thought of as tech heavyweights often have more in common with traditional economy players from a business model standpoint: the former just happens to use newer technologies and find ways to make them useful for people.

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.[3] Further, we are committed to promoting proactive approaches to ensuring end-user privacy and note our endorsement of the National Telecommunications and Information Administration's (NTIA) support for privacy-by-design approaches.[4]

As regulators from across key markets abroad continue to rush to utilize approaches to regulation of 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 great barriers to bringing novel products and services to market—slowing technological innovations to the pace of government approval.

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

[3] *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.

[4] RFC at 48602.

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 to provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation. NIST's Privacy Framework can and should inform this approaching legislative process.

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. Small businesses represent 99.7 percent of all U.S. firms,[5] and they require heightened assistance and must play a more significant role in the development of privacy management strategies. It is important that NIST remain mindful of the fact that large companies often dedicate large budgets to create and maintain privacy control processes and have the ability to hire staff and consultants to mitigate privacy risks, while small enterprises very often do not. For many of our members, the role of chief privacy officer may be one of five hats worn by a single employee. The essential role of American small businesses, along with the unique resource constraints they face, make the NIST Privacy Framework even more important.

Like the NIST Cybersecurity Framework, we urge NIST to ensure that its Privacy Framework provides a scalable, flexible, voluntary toolbox that any organization can use. However, we note that our 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.

While we support the Privacy Framework being developed as a comprehensive guide, we also urge NIST to further develop a deliverable to define the fundamentals of a small business-focused Privacy Framework (much like what NIST developed for the NIST Cybersecurity Framework[6]). In addition, the Federal Trade Commission (FTC) develops best practices in the form of its Start with Security guide for SMEs, which draws from the NIST Framework,[7] and we encourage NIST to work with the FTC in a similar campaign to assist small businesses in addressing privacy.

[5] https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.
[6] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.
[7] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

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 make the business case (i.e., it provides a return on investment) for using the future Privacy Framework. The App Association is able to encourage use of the future NIST Privacy Framework throughout our community in a few key ways, including direct member education and public-private partnerships like the Information Technology Sector Coordinating Council. We commit to working closely with NIST and other public and private stakeholders to develop and help implement more small business-focused privacy risk management practices that support the growth of the digital economy.

Further, in response to specific minimum attributes proposed by NIST and high-priority gaps the Privacy Framework could address, the App Association offers the following input:

- We support each of the seven minimum attributes suggested by NIST for the Privacy Framework, particularly #3 (Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses).
- We support NIST taking a technology-neutral approach in developing the Privacy Framework.
- We agree that the Privacy Framework should be scalable and flexible so as to avoid advancing overbroad or heavy-handed approaches to privacy, and to promote customizable approaches to improving privacy. The Framework should be able to be applied to any sector, even if that sector already faces sector-specific privacy regulation.
- With regards to NIST's request for input on core privacy practices that are broadly applicable across sectors and organizations, we urge NIST to review the App Association's *App Privacy Essentials*, a web-based resource the App Association created for small business digital economy innovators to assist them in developing their approach to privacy and their public privacy policies, available at https://actonline.org/app-privacy-essentials/. This resource also includes guidance for our members that operate in sectors that require further specific steps to be taken (e.g., apps for children, health and wellness, and financial).

- With regard to NIST's request for high-priority gaps for which privacy guidelines, best practices, and new or revised standards are needed and that could be addressed by the Privacy Framework or a related roadmap:
    - We urge the future Privacy Framework to advance privacy-by-design from the earliest stages of product design.
    - We urge the Framework to address privacy research as a crucial component of sound federal privacy policy. Emerging methods of providing products and services that use large amounts of data demand creative experimentation with privacy models. Meanwhile, privacy experts often employ a hypothetical or normative view of how consumers *should* behave when presented with privacy choices—or a lack of privacy choices—connected to the services or products with which they are interacting at a given moment. We believe this theoretical approach is employed too often and that empirical evidence would go some way toward ameliorating policy outcomes that otherwise suffer from being based on theoretical or aspirational assumptions.
- We also urge NIST's development of a Privacy Framework to happen in coordination with other key efforts, both within the federal government and elsewhere, to develop privacy requirements and/or guidance. NIST should ensure its coordination with NTIA's development of a privacy framework and various sector-specific efforts (e.g., Department of Health and Human Services' development of guidance on compliance with the Health Insurance Portability and Accountability Act of 1996). Further, NIST's Privacy Framework should align with and help advance key international privacy constructs, including the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System and the EU-U.S. Privacy Shield.

The App Association supports NIST's development of a 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 working with NIST and other stakeholders on developing an environment that protects privacy, prosperity, and American economic leadership.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

ACT | The App Association