
January 14, 2019

Via Electronic Mail

The Honorable Walter G. Copan
Under Secretary of Commerce for Standards and Technology and
Director of NIST
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Comments on *Developing a Privacy Framework*
Docket No. 181101997–8997–01 (November 14, 2018)
Notice of Extension (December 17, 2018)

Dear Dr. Copan:

The Fashion Innovation Alliance (FIA) submits these comments to the Department of Commerce, National Institute of Standards and Technology (NIST) in response to the Notice and Request for Information on *Developing a Privacy Framework*, published in the *Federal Register* on November 14, 2018.[1]

The Fashion Innovation Alliance (FIA) was founded in 2016 to provide a platform and voice for leaders working at the intersection of design, retail and technology. These innovators include startups and established brands developing smart products, digital commerce platforms and emerging technologies in retail. FIA is the first organization to address global policy and regulatory compliance, access to capital, inclusion and innovation in fashion tech and beauty tech — from the lens of creative visionaries on both sides of the Atlantic.

[1] Developing a Privacy Framework, 83 Fed. Reg. 56,824 (Nov. 14, 2018).

**Discussion**

The Fashion Innovation Alliance welcomes the opportunity to comment on the development of the Privacy Framework, especially given the emerging technology trends and innovation in connected products, digital commerce and retail. FIA values the privacy of the consumers using connected products and services, and we recommend that any new policies or best practices help create a flexible environment for technologies shaping innovation at the intersection of design, retail and technology.

Data has been repeatedly termed "the new oil," having tremendous value to both brands and consumers. Data has the power to create meaningful change across industries. Well-managed consumer data allows more relevant product and movie recommendations, smart apparel that responds to body temperature and movement, and the ability to simply stay engaged with shoppers. And while it's important for entities to address transparency in their data practices, designing privacy protections with an ethical approach will be key to building long-term trust with consumers. As noted in NIST's Request for Information, new technologies "are giving rise to increased concerns about their impacts on individuals' privacy."[2] But privacy is not just about responding to the latest technologies, privacy is also about how humans interact with each other in a data-driven world.

**Stakeholder Diversity Across Sectors**

We appreciate NIST's efforts in including panelists and experts from industry, civil society and academia during the first Privacy Framework workshop. Diversity of thought is an important part of the stakeholder process, but it is also critical that stakeholders participating in NIST's Privacy Framework process reflect diversity across sectors — from technology and telecommunications to art and design, as well as retail and hospitality.

We have seen how the cross-disciplinary exchange typical of companies working at the intersection of art, design, retail and technology not only drives innovation, but also leads to advancements that help humanity. These include companies designing sensor technology glasses to help fight Parkinson's disease, AI-enabled devices to detect counterfeit products and connected clothing that gives users control over their personal data.

**Addressing the Human Element and Privacy Risks Across the Supply Chain**

While entities often focus on the security features and privacy policies vetted by their legal teams, the human element — at every stage of an organization's supply chain — is the most powerful part of protecting individuals' personal privacy. This includes company experts across the

[2] 83 Fed. Reg. 56,824 (Nov. 14, 2018).

organization's entire ecosystem — from designers and manufacturers developing connected products to the consumers using products and sharing their data. Individuals working for business-to-business (B2B) companies should also be aware of the privacy risk environment of the end-users, including how third parties access individuals' personal data and how real-time location and other sensitive data is collected and sold.

Also, as more companies take a direct approach in setting up and managing their supply chains for trade and transparency purposes, it's critical that they work with their suppliers to better assess and manage the privacy risks. In the same way that effective supply chain management can help organizations build trust and transparency for sustainability and ethical sourcing, effective privacy protections across suppliers can also help build trust in a company's products and services.

The human element also extends to the companies' employees — who may be placed in compromising positions at certain times to share data with unauthorized third parties. For example, within the fashion tech community, we have witnessed professionals attempting to collect and analyze personal data of fashion tech leaders and consumers — some directly asking for customer and client lists and others using more cunning tactics to get personally identifiable information. While an employee may consider the person requesting such data to be a friend or colleague, the person still has an ethical duty not to share such data.

For these reasons, FIA recommends that the Privacy Framework address guidelines on communicating and developing privacy protections across an entity's supply chain. The guidelines should also address practices in dealing with an organization's existing suppliers, contractors as well as professionals seeking to do business with the organization.

**Innovative and Inclusive Workforce of Privacy Professionals**

NIST has requested comments on "How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations."[3]

Privacy and data security professionals are key to ensuring that both the public and private sectors are able to implement and effectively manage privacy practices, especially as the technologies and data protection challenges continue to evolve and change.

The current challenges for a diverse and inclusive pool of senior privacy professionals are also clear. During a September 2018 privacy hearing before the Senate Commerce Committee, the

[3] 83 Fed. Reg. 56,824, 56,826 (Nov. 14, 2018).

witnesses representing tech and telecom included one woman and not a single person of color.[4] This is important to note and remedy because a lack of diversity at the top levels of the industry suggests there are cultural blind spots within these entities that may leave underrepresented segments of the population at increased risk for privacy breaches.

FIA recommends that the Privacy Framework include best practices and encourage companies to not only address overall hiring and retention efforts, but also ways to include diverse voices at all levels — including attorneys specializing in privacy and data security, experts in data ethics and technologists.

FIA also recommends that when addressing human talent for privacy functions, that NIST incorporate ethics as part of the discussion. Given the recurring incidents of the mismanagement of data across online platforms and services, recruiting and retaining talent with expertise in privacy and ethics will help companies better navigate social and business issues. Over the past year, citizens around the world have witnessed the devastating effects when companies do not respect human data and the users of their products and services. Weaving ethics into privacy discussions around talent and data will help to improve trust and transparency in the products and platforms powered by such companies.

**Conclusion**

The Fashion Innovation Alliance appreciates the opportunity to submit these comments and would be happy to provide you with additional information or clarification. For the reasons stated above, the Alliance respectfully requests that the federal government continue to collaborate and work with entities across sectors when developing the Privacy Framework, and also include ethics as part of the global privacy discussion.

Respectfully submitted,

Kenya N. Wiley
Founder and CEO
Fashion Innovation Alliance

[4] *Examining Safeguards for Consumer Data Privacy*: Hearing before the U.S. Senate Committee on Commerce, Science and Transportation (2018).