w i r e w h e e l

1310 N. Courthouse Rd, Suite 200, Arlington, VA 22201
(202) 750-0634 | info@wirewheel.io | https://wirewheel.io

January 14, 2019

Re: Request for Information for the NIST Privacy Framework

WireWheel Inc., is pleased to respond to this Request for Information to help guide development of the NIST Privacy Framework.

By way of background, WireWheel provides data privacy and data protection as-a-service. Our Privacy and Data Protection Platform supports all phases of a global privacy management and compliance program, uniquely addressing requirements around personal data inventory and mapping, collaboration, vendor risk management, third party compliance, and more. Our comments here are informed by our experience with companies, government regulators, and other entities over the last few years, where we have seen first-hand the difficulties that the regulators face in deciding how to regulate this space, and that the companies face in responding to the uncertain and varied regulation regime around the world. WireWheel leadership team includes CEO Justin Antonipillai, former Acting Undersecretary of Economic Affairs at the US Department of Commerce in the Obama administration and lead US Negotiator of the EU-US Privacy Shield; Chief Scientist Dr. Amol Deshpande, Professor at University of Maryland at College Park and a leading expert on big data platforms and collaborative data science; CTO Ed Peters, formerly CTO at Opower, a large public company; and Chief Product Officer Chris Getner, a machine learning expert.

We believe that it is critical for NIST to develop a comprehensive Privacy Framework, analogous to the highly successful Cyber Security Framework. Privacy and data protection now go hand-in-hand with cybersecurity, and have become critical risk, strategic, customer, sales, and compliance issues for companies around the world. We have seen other countries take a leadership role on this issue, and NIST can play an important role in increasing the US engagement in this issue. Moreover, differences in global regulations have led to uncertainties that impact innovation as companies are not able to properly utilize their data in a responsible, ethical, and privacy-conscious manner. A NIST framework would help spur further innovation and help US companies take leadership in this space again.

Establishment of a Privacy Framework has become especially important in recent years with increasing adoption of Internet of Things (IoT), Artificial Intelligence (AI), and Biometric Data. In isolation, any specific IoT data item may seem innocuous, but in the aggregate, IoT data can be highly indicative of many extremely personal and sensitive personal attributes. IoT data is also collected in a distributed and decentralized manner, and is communicated in an ad hoc manner.

A NIST framework that sets guideposts for consideration of these issues could also help establish privacy-conscious architectures in this space. Similarly, increased use of AI has led to significant ethical issues that fall under the purview of this topic; this is because personal data is often used to design and learn models that are then used to make inferences about the personal attributes of people. A framework that systematically evaluates the risk in incorporating AI in business processes is thus sorely needed. Finally, there have been many high-profile situations where biometric data (e.g., DNA) has been used in unintended ways. This will become more and more common with the prevalence of devices like smart watches that can monitor and manage health data. Although some of this data is covered by existing regulations like HIPAA, a comprehensive framework that handles all personal data would make it easier for companies to understand how to combine and manage different types of such information.

Finally, a comprehensive Privacy Framework will also allow companies like WireWheel to design platforms and products to help with transparency and compliance. The large number of slightly different and sometimes incompatible standards and regulations has made compliance very complicated, has hurt innovation in Data Governance and Data Ethics tools, and is starting to negatively impact the overall ecosystem of Big Data tools.

In our opinion, a comprehensive privacy framework established by NIST should be non-prescriptive and include the following:

- The framework should help companies make better determination of what constitutes “personal data.” Many recent regulations have taken a broad view of this term, but we still see significant emphasis (especially in US) on clearly-identified attributes such as Name, Address, Government Identifiers, Mobile Device IDs, and IP Addresses. It is crucial to broaden the definition to include other categories of personal information so that risk can be quantified more appropriately. Moreover, the distinction between “anonymous” data (i.e., data that cannot be tied back to an individual) and “pseudonymous” data (i.e., data that doesn’t contain identifiers but could be re-identified) needs to be made clearer. The framework should also provide guidance on how to treat data that collectively belongs to a small group of individuals (e.g., a household).
- The framework should identify how companies can implement standard “privacy-by-design” principles including data and access minimization, encryption, anonymization and pseudonymization, and others. Coordination with the proposed ISO Standard on Privacy by Design should be considered.
- The framework should identify what companies should consider regarding data transfers and data sharing across organizations through publicly-available APIs, ad hoc file transfers, or other mechanisms. The rise of specialized services and ease of data communication have led to these practices being widely adopted. Clearly identifying which companies the data is being shared with, and the nature of the data being shared, are both crucial in this context. Data ownership issues are often unclear in such settings, especially as data undergoes various transformations and may be combined with other

pieces of information with different provenance. The trade implications of data transfer issues have also become a real, but manageable issue, given the right approach.

- The framework should be outcomes-based, with different sets of outcomes focused on the individuals and the companies. From an individual's perspective, some of the key outcomes include: Does an individual have sufficient rights to the data, especially data that has been collected from the individual without their knowledge, or inferred about them? Is an individual able to obtain transparency into where their data went? Are they able to take their data wherever they want? On the other hand, from a company's perspective, some specific outcomes may be: Can a company quickly locate all data for an individual, especially without well-defined IDs? Can it delete all the information for an individual without undue hardship? Is it able to follow up with all the partners to whom they sent personal data for an individual and able to understand the provenance of any specific piece of data that it has about an individual?

We welcome the opportunity to further participate in the development of a comprehensive NIST framework.

Sincerely,

Dr. Amol Deshpande, PhD
Chief Scientist
WireWheel, Inc.