U.S. Technology
Policy Committee

January 14, 2019

Submitted Electronically

Mr. Kevin A. Kimball, Chief of Staff
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Comments on "Developing a Privacy Framework" (Docket 181101997–8997–01)

Dear Mr. Kimball:

ACM, the Association for Computing Machinery, is the world's largest and longest established association of computing professionals, representing approximately 50,000 individuals in the United States and 100,000 worldwide. ACM is a non-profit, non-lobbying and non-political organization whose U.S. Technology Policy Committee (Committee) is charged with providing policy and law makers throughout government with timely, substantive and apolitical input on computing technology, and the legal and social issues to which it gives rise.

The Committee believes that both rigorously developed guidance and statutory requirements are needed to safeguard personal privacy of U.S. citizens. We thus applaud the National Institute of Standards and Technology (NIST) for release of its recent Request for Information (RFI) on "Developing a Privacy Framework."[1] In response, we are pleased to timely submit:

- for NIST's general consideration, our March 2018 "*Statement on the Importance of Preserving Personal Privacy*," which outlines ten guiding principles for its protection; and

- the following Comments specific to NIST's RFI addressing six of the 26 topics that the RFI presents for discussion.[2]

For ease of reference, each such topic is numbered and labeled below as in the RFI.

[1] 83 Fed. Reg. 56824 (November 14, 2018) as modified by 83 Fed. Reg. 64531 (December 17, 2018).

[2] This document is a product of the ACM U.S. Technology Policy Committee (USTPC). It was prepared by the following USTPC members. Its principal authors are: Brian Dean, Secureworks (Chair, USTPC Privacy Subcommittee); Dr. Lorraine Kisselburgh, Purdue University (Chair, USTPC Social Media Privacy Working Group); Stuart Shapiro, USTPC Past Chair; and Arnon S. Rosenthal, USTPC Privacy Subcommittee Member.

Organizational Considerations

1) Greatest challenges in improving organizations' privacy protections for individuals . . .

The Committee perceives four principal and overarching challenges within enterprises and organizations to establishing satisfactory privacy protections:

a) “Privacy-by-design” insufficiently informs product development.

Internal development cycles for producing applications and technologies, often rapidly under significant market pressures, frequently are geared purely or predominantly to create functionality and thus inherently lack incentives for protecting individuals’ privacy. Consequently, privacy protection in the form of express initial consideration of how data collected will be used and/or shared by the product too often is omitted from the critical early stages of these processes or becomes a costly afterthought that is incompletely addressed late in the development cycle as deadlines loom.

b) Data commodification is an integral driver of many business models.

Data collection and commodification (often on an enormous scale) has become an entrenched global business model, supported and driven by large technology investments. Government at multiple levels, also collects, retains and shares large quantities of data, although generally for non-economic reasons. While such comprehensive data collection, retention and sharing clearly benefit the collector, individual subjects who come to object[3] to these actions at times have little leverage to change them as a practical matter beyond foregoing use of a given technology or service entirely.[4]

While formally documenting data flows (including to third parties) can add a degree of transparency, actually restricting corporate data access and use necessarily will require altering business models, forgoing opportunities, and redesigning applications, interfaces, and infrastructures. Lucrative current practices thus are unlikely to be abandoned without new external influences, such as: regulatory incentives, creation of an independent data protection authority; and/or significant continued consumer protest and behavior self-modification.

[3] Many consumers tend to focus on product convenience and utility until they learn of the types and amounts of their data collected, often without their knowledge, and the many purposes for which that data is used.

[4] Indeed, as widely reported, even where a product nominally affords “control” options, these can be less robust than suggested or even wholly inoperative.

c) Successfully balancing all stakeholders' interests will be complex and difficult.

Efforts to identify and codify "universal" privacy principles extend back decades[5] and remain ongoing at this writing, most recently and dramatically evidenced by adoption of Europe's General Data Protection Regulations and calls gaining substantial currency in the United States for passage of comprehensive consumer privacy protection legislation. As reflected in our attached *Statement on the Importance of Preserving Personal Privacy*, ideally, data collectors in all sectors at minimum would acknowledge and implement baseline privacy principles that: clearly and concisely articulate when, what and why data is collected; how it is used; the duration for which it is retained; how it is protected; and how inaccurate data can be expunged or corrected.

In addition to embracing and employing such guiding principles, industry policy and practice should be based upon a clear and broadly accepted definition of personally identifiable of information (PII) specified in NIST's intended Framework. That document also should delimit permissible uses PII, including particularly how such data may be reused when de-identified, and how individuals can restrict sharing of their own data.

The Committee understands that, realistically, these goals are likely to be only partially met. A privacy Framework, however, can help achieve them to the greatest extent possible by endorsing specific privacy doctrines and, more specifically, by benchmarking detailed assessment criteria and metrics for gauging the degree to which critical goals are being met. The Committee hopes that its attached *Statement on the Importance of Preserving Personal Privacy* will be of use and interest to NIST in this context.

5) Current policies and procedures for managing privacy risk . . .

To succeed, efforts to manage privacy risk must: be ongoing and routine; adhere to industry standards and best practices; seek to improve those standards and practices when inadequate or underdeveloped; and incorporate independent audits and appropriate risk models. A NIST Framework can assist in meeting these requirements by:

- Crafting an effectively universal definition of protected personal data that includes explicit, contextual definitions just as, we note, HIPAA, GBLA, and GDPR all have done in their spheres;

- Identifying regular, independent, and reliable privacy-promoting practices concerning personal data access, use, and controls (*e.g.*, protection, destruction). Such specified practices should include the formal documentation of: data flows; collection

[5] The Organization for Economic Co-operation and Development did its seminal work in 1980.

- points; downstream users and uses of the data (including by third parties);[6] and how/why data (not merely personal data) is used. Indeed, the Framework effort productively might go so far as to encompass the promulgation of standard notation formats and templates to assist organizations with implementation;

- Affirming that, to meet acceptable standards of privacy protection, companies must report data privacy breaches as quickly as possible. Defined reporting deadlines, and penalties for lack of compliance, also must be part of any such regime for it to be effective; and

- Endorsing risk-based policies and procedures for protecting personally identifiable information from unauthorized disclosure, misuse, improper alteration and inappropriate deletion.

12) Mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices . . .

For the reasons discussed above, without clear privacy-protection mandates (whether internally developed or externally imposed), product development teams will tend to prioritize innovation and speed to market over privacy protection. Effective incentives to privacy-protective voluntary action thus are important counterbalances to these tendencies. Defining and publicizing standard metrics is a critical prerequisite to helping organizations improve privacy protection. They also can facilitate appropriate compliance and enforcement actions in specific circumstances.[7]

Specific Privacy Practices

22) Practices … most critical for protecting individuals' privacy . . .

The effective protection of individuals’ privacy will require somewhat different practices by consumers, businesses and government. However, the applicable guiding core principles – the importance of which can constructively be elevated by the proposed Framework – cut across these environments. They are:

[6] We specifically recommend that NIST propose that data collectors maintain (and where possible make public) auditable lists of third parties with which data is shared that include details of data attributes, collection dates, collection purposes, and intended retention.

[7] Indeed, new statutes and regulations might productively make explicit that the fact of compliance with specific privacy principles and practices may be offered as a defense to liability in delineated circumstances.

- Transparency: Businesses must effectively educate consumers in easy to understand data management principles and methods applicable to their products so consumers can make informed decisions about when to provide personally identifiable information (PII), and how to effectively opt out of its use or distribution. Government, for its part, also must clearly identify what PII it collects and why and consumers themselves must be educated about the practical importance of "privacy hygiene."

- Data Collection/Use Limits: Enterprises and government must limit the collection of PII and minimize its retention by, for example, only acquiring and retaining data essential to provide service to active clients.

- Minimization: Private and government sector actors must be required to mitigate the risk of PII breaches by minimizing the identifiability of data created, collected, and retained regardless of how minimal or briefly held that data is. Individuals also should be informed that, in many cases, it may not be essential to provide PII simply because it's requested.

- Data Security: Actors in all data ecosystems must take affirmative steps (*e.g.*, using strong encryption) to safeguard PII to prevent its inappropriate access and use.

25) Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence . . .

The practices addressed by the RFI and central to the production of an effective Framework are perhaps even more relevant to the Internet of Things (IoT) than to existing technologies because of the tremendously enhanced vulnerability of IoT devices to negative externalities, such as botnets. Moreover, because the application opportunities for IoT technology are seemingly endless, it is important to recognize that many IoT devices rely on ongoing data collection and analysis to improve their performance. Often this data is PII.

The massive amount of personal data collected, often unbeknownst to the user, can lead to collateral damage from a variety of actors, including the vendor who collects the data or thieves who pilfer the data from the devices or the databases they feed. The potential for government access and misuse of the data also exists. In the artificial intelligence context, the massive data sets that power machine learning algorithms and the collection and storage of information also create the potential for serious breaches of personal privacy that production of the Framework is intended to mitigate.

Conclusion

ACM's U.S. Technology Policy Committee looks forward to technically assisting NIST and others throughout the process of developing, refining and potentially codifying enhanced public privacy protections and welcomes any and all inquiries to that end. For further information or additional clarification, please contact ACM Director of Global Policy and Public Affairs Adam Eisgrau at 202-580-6555, or eisgrau@acm.org.

Sincerely,

James A. Hendler, Chair

usacm ACM US Public Policy Council

Association for Computing Machinery (ACM)
ACM US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

March 1, 2018

USACM STATEMENT ON THE IMPORTANCE OF PRESERVING PERSONAL PRIVACY

USACM believes that the benefits of emerging technologies, such as Big Data and the Internet of Things, should and need not come at the expense of personal privacy. It is hoped and intended that the principles and practices set out in this Statement will provide a basis for building data privacy into modern technological systems. USACM encourages the development of innovative solutions to achieve these goals.

Foundational Privacy Principles and Practices

Fairness

- An automated system should not produce an adverse decision about an individual without the individual's full knowledge of the factors that produced that outcome.

Transparency

- Provide individuals with clear information about how and by whom their personal data is being collected, how it will be used, how long it will be retained, to whom it may be disclosed and why, how individuals may access and modify their own data, and the process for reporting complaints or updates.
- Where feasible, provide these details prior to data collection and creation.
- Ensure that communications with individuals (*i.e.*, data subjects) are comprehensible, readable, and straightforward.

Collection Limitation and Minimization

- Collect and retain personal data only when strictly necessary to provide the service or product to which the data relates, or to achieve a legitimate societal objective.
- Minimize the identifiability of personal data by avoiding the collection of individual-level data when feasible, and taking into account the risk of correlation across data sets to re-identify individuals.

Individual Control

- In all circumstances, consent to acquisition and use of an individual's data should be meaningful and fully informed.
- Provide individuals with the ability to limit the collection, creation, retention, sharing and transfer of their personal data.
- Ensure that individuals are able to prevent personal data obtained for one purpose from being used or made available for other purposes without that person's informed consent.
- Provide individuals with the ability to access and correct their personal data.

Data Integrity and Quality

- Ensure that personal data, including back-up and copies forwarded to third parties, is sufficiently accurate, current, and complete for the purpose for which it is to be used.
- Conduct appropriate data quality assessments.

Data Security

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
- Audit access, use, and maintenance of personal data.

Data Retention and Disposal

- Establish clear policies with fixed publically stated retention periods and seek individuals' affirmative consent to retain their data for longer periods.
- Store personal data only for as long as needed to serve the stated purpose for its initial collection.
- Where feasible, de-identify personal information until properly destroyed.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including back-up data and information shared with third parties.

Privacy Enhancement

- Promote and implement techniques that minimize or eliminate the collection of personal data.
- Promote and implement techniques that ensure compliance with the best privacy practices as they evolve.

Management and Accountability

- Ensure compliance with privacy practices through appropriate mechanisms, including independent audits.
- Establish and routinely test the capability to address a privacy breach or other incident.
- Implement privacy and security training and awareness programs.

Risk Management

- Routinely assess privacy risks to individuals across the data life cycle using appropriate risk models.