November 8, 2018

By Electronic Mail

David J. Redl
Assistant Secretary for Communications and Information
United States Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Comments on "Developing the Administration's Approach to Consumer Privacy"

Dear Assistant Secretary Redl:

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 US Technology Policy 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.

On behalf of the Committee, and in response to the National Telecommunications and Information Administration's September 26, 2018 request for public comment in Docket 180821780–8780–01 (RIN No. 0660–XC043), I am pleased to submit the attached *Statement on the Importance of Protecting Personal Privacy* of March 2018[1] for NTIA's consideration and guidance in connection with development of the Administration's approach to consumer privacy. In addition, we respectfully and specifically commend the agency's attention to the following principles and practices articulated in that Statement and elaborated upon in written testimony of July 2, 2018 provided to the Senate Commerce Committee's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security:[2]

[1] *See* www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf
[2] *See* www.acm.org/binaries/content/assets/public-policy/usacm/usacm_senate_facebook_hearing_statement_transmittal.pdf

ACM U.S. Technology Policy Committee
1701 Pennsylvania Ave NW, Suite 200
Washington, DC 20006

+1 202.580.6555
eisgrau@acm.org
www.acm.org/public-policy/ustpc

1. **Limit collection and minimize retention of personal data[3]**
   - Collect and retain only personal data essential for the collector to provide its service or product.
   - Collect data only from active account holders (or members).
   - Mitigate the risk of privacy breaches by minimizing the identifiability of data collected or retained, regardless of how minimal or briefly held.

2. **Clarify and simplify user consent processes and maximize user control of data**
   - Provide individuals with easily understood and centrally accessible consent options specific to the type, scope, and purpose of data use to assure users' meaningful and fully informed consent.
   - Allow users to easily limit the collection, creation, retention, sharing, and transfer of personal data.
   - Prevent personal data obtained for one purpose from being used or made available for other purposes without fully informed consent.
   - Encourage research into and the development of smart, automated privacy agents to infer privacy preferences, establish smart defaults, and scaffold decisions about consent and disclosure.

3. **Simplify data sharing policies and assure transparency in data flows**
   - Provide individuals, prior to data collection and creation, with clear and concise information about: how and by whom their personal data is collected; how it will be used; how long it will be retained; to whom and why it may be disclosed; and how they may access, modify, and delete their data.
   - Maintain an auditable list of third parties with whom each person's data has been shared, including what was shared and for what purpose(s).
   - Incorporate visualization tools into platform designs to enhance users' understanding of how their data are being used.

4. **Clearly define and disclose data ownership terms and attendant rights**
   - Clarify data ownership boundaries, including who owns data that is collected and used to support platform interoperability, platform engagement, and platform support.
   - Develop binding best practices to assure transparency about data sources, so that users and authorities can determine the origin of data and bar the use of data unlawfully acquired.

5. **Adopt and enforce data security practices commensurate with risk**
   - Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
   - Audit the access, use, and maintenance of personal data.
   - Report data privacy breaches as quickly as possible.

[3] "Data" is used here to include personal information, patterns of individual behaviors, identifying imagery, and spatial presence.

6. **Require clear, fair, and responsible data access, retention, and disposal policies**
   - Establish clear policies with fixed, publicly-stated retention periods and seek affirmative consent to retain personal data for longer periods, if needed.
   - Reduce the risk of data loss by using de-identification, aggregation, encryption, and other methods to reduce the data's accessibility.
   - Implement an auditable process for verifying that data has been deleted when requested, including data provided to third, fourth, and other downstream parties.
   - Implement mechanisms to promptly destroy unneeded or expired personal data, including backup data and information shared with third and other downstream parties.

7. **Codify appropriate and meaningful oversight of third party developer platforms (API)**
   - Publish clear guidelines for app developers regarding acceptable and unacceptable uses of data.
   - Require oversight, review, and enforcement of policies regarding the types of apps and uses of data that are allowed, with clear consequences for misuse.
   - Ensure that the terms of service for all applications deployed on, by or through a platform are consistent with the platform's own data use policies.

8. **Enable and support legitimate and appropriately overseen platform research**
   - Design platforms to facilitate robust research access.
   - Encourage platforms to publish guidelines for researchers detailing: acceptable use of data, procedures for protecting user privacy, data retention practices, and other expectations of those conducting research on the platform.
   - Allow researchers to submit evidence of approval for studies that have been reviewed by institutional review boards or other appropriate human subjects protection boards.
   - Enforce consequences for conducting unauthorized research studies and/or failing to adhere to published guidelines.

9. **Measure the actions and omissions of companies against all appropriate ethical standards, including ACM's Code of Ethics. The Code affirms that all computing professionals should:**
   - Contribute to society and to human well-being working to minimize the negative consequences of systems, and ensure their developments will be used in socially responsible ways. (ACM Code *§1.1*)
   - Avoid harm to others, where harm includes "negative consequences" or the "undesirable loss of information or property." (ACM Code *§1.2*)
   - Respect privacy by only using personal data for legitimate ends and without violating the rights of individuals and groups. (ACM Code *§1.6*)
   - Consider and mitigate the possible risks of the systems they develop. (ACM Code *§2.5*)
   - Ensure that the public good is a central concern. (ACM Code *§3.1*)
   - Provide responsible stewardship of systems embedded in society. (ACM Code *§3.7*)

Finally, the Committee wishes to underscore its full agreement with (and appreciation for NTIA's articulation of) "high level goal" number six concerning how critical it is and will increasingly become for the nation to "incentivize privacy research."[4]

ACM's US Technology Policy Committee looks forward to technically assisting NTIA 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 should you have any other questions, 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

Attachment: *Statement on the Importance of Protecting Personal Privacy* (March 2018)

[4] "The U.S. Government should encourage more research into, and development of, products and services that improve privacy protections. These technologies and solutions will include measures built into system architectures or product design to mitigate privacy risks, as well as usability features at the user-interface level. These innovations require more research into understanding user preferences, concerns, and difficulties, as well as an understanding of the impact on legal obligations of third parties and the ability of third parties to exercise other rights provided by law. Privacy research will inform the development of standards frameworks, models, methodologies, tools, and products that enhance privacy." 83 Fed. Reg. 48602 (Sept. 26, 2018)

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.

ACM US Public Policy Council
1701 Pennsylvania Ave NW, Suite 200
Washington, DC 20006

+1 202.580.6555
acmpo@acm.org
usacm.acm.org