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

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

April 9, 2018

Hon. John Thune, Chair
United States Senate
Comm. on Commerce, Science & Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Hon. Charles Grassley, Chair
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Hon. Bill Nelson, Ranking Member
United States Senate
Comm. on Commerce, Science & Transportation
425 Hart Senate Office Building
Washington, DC 20510

Hon. Dianne Feinstein, Ranking Member
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Committee Consideration of Facebook Data Compromises and Related Issues

Dear Senators Grassley, Thune, Feinstein and Nelson:

ACM, the Association for Computing Machinery, is the world's largest and oldest association of computing professionals representing approximately 50,000 individuals in the United States and 100,000 worldwide. Its US Public Policy Council (USACM) 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 USACM, thank you and the Committees for undertaking a full and public exploration of the causes, scope, consequences and implications of the enormous breaches of privacy and public trust resulting from Facebook's and outside parties' use and misuse of vast amounts of Facebook users' and millions of others' data. The technical experts we represent – including luminaries in computer science, engineering and other computing disciplines – stand ready to lend their expertise to you and your staffs at any time as the hearing and legislative processes progress.

USACM believes that the issues raised by this incident, and the intense scrutiny now appropriately being brought to bear on it, make this a watershed moment. The issue and challenge is not merely how to address the failings of a single company, but to understand how privacy and trust in an era of big data, pervasive networks and socially embedded platforms must be addressed in order to promote the public interest broadly in our society, including specifically the integrity of our democratic institutions.

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

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

As your Committees prepare to convene, USACM offers the following broad observations grounded in our technical understanding and commitment to the highest ethical standards in our professional practice:

- It is critical to understand the full scale and consequences of how Facebook's past and present business practices or failures compromised, and may continue to undermine, users' and others' privacy and data security. It is also critical, however, to understand the technology underlying its actions and omissions so that truly effective technical and legal means may be designed to assure the protection of privacy by limiting data collection and sharing, ensuring real user consent and notice, and providing full transparency and accountability to its community members. These and other fundamental principles are detailed in USACM's 2018 *Statement on the Importance of Preserving Personal Privacy* (attached);

- The actions and omissions already confirmed or publicly acknowledged to have occurred by Facebook appear to stem from systemic deficiencies in a range of processes considered essential by computing professionals, including proactive risk assessment and management, as well as protecting security and privacy by design;

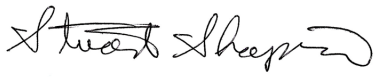
- Facebook's actions and omissions should be measured against all appropriate ethical standards. The first principle of ACM's long-established Code of Ethics states that, "An essential aim of computing professionals is to minimize negative consequences of computing systems . . . and ensure that the products of their efforts will be used in socially responsible ways." Adhering to broadly accepted social norms the ethical code also requires that computing professionals "avoid harm to others," where harm includes injury, negative consequences, or undesirable loss of information or property.

- The present controversy underscores that we are living in an era of mega-scale data sets and once inconceivable computational power. Consequently, the nature, scale, depth and consequences of the data, technical and ethical breaches understood to have occurred thus far in the Facebook case are unlikely to be confined to a single company, technology or industry. That argues strongly for Congress to comprehensively revisit whether the public interest can adequately be protected by current legal definitions of consent, the present scope of federal enforcement authority, and existing penalties for breach of the public's privacy and trust on a massive scale; and

- Size and power are not the only consequential hallmarks of the new information era. Ever more complicated and multiplying synergies between technologies (such as platform architecture, data aggregation, and micro-targeting algorithms) exponentially increase the vulnerability of personal privacy. Similarly increasing complexity in the ways that social media continues to be woven into modern life amplifies the threat. Together these trends make it clear that addressing separate elements of this rapidly changing ecosystem in isolation is no longer a viable means of protecting the public interest. Rather, we urge Congress to consider new and holistic ways of conceptualizing privacy and its protection.

Thank you again for your work at this pivotal time and for formally including this correspondence and the attached *Statement* in the record of your upcoming hearing. USACM looks forward to assisting you and your staffs in the future. To arrange a technical briefing, or should you have any other questions, please contact ACM's Director of Global Public Policy, Adam Eisgrau, at 202-580-6555 or eisgrau@acm.org.

Sincerely,



Stuart Shapiro, Chair

Attachment

cc: Members of the Senate Commerce and Judiciary Committees

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.