Association for Computing Machinery (ACM)
US Technology Policy Committee (USACM)

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

July 2, 2018

Hon. Jerry Moran, Chair
United States Senate
Comm. on Commerce, Science, and Transportation
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security
521 Dirksen Senate Office Building
Washington, DC 20510

Hon. Richard Blumenthal, Ranking Member
United States Senate
Comm. on Commerce, Science, and Transportation
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security
706 Hart Senate Office Building
Washington, DC 20510

Re: Recommendations and Call for Action to Address Data Privacy Risks and Harms Revealed by Facebook/Cambridge Analytica Inquiries

Dear Chairman Moran and Ranking Member Blumenthal:

ACM, the Association for Computing Machinery, is the largest and longest-established association of computing professionals in the world, representing approximately 50,000 individuals in the United States and 100,000 globally. USACM is the organization's U.S. Technology Policy Committee, charged by ACM 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.

We do so today in the form of the attached statement respectfully and timely submitted for the record of the Subcommittee's hearing on "*Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks,*" conducted on June 19th. In our attached letter of April 9 (entered into the record of the full Committee's joint hearing with the Judiciary Committee of April 10 and Appendix A to the attached Statement),* we urged "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."

In candor, we believe that early recommendation to have been too conservative to fully serve the public interest. USACM thus now concludes and recommends in the attached statement that "[g]iven the significance of the privacy and ethical shortcomings" brought to light by the joint Committees' and Subcommittee's inquiries, "now is the time for Congress to act to protect the public interest and the integrity of the democratic process by adopting comprehensive and effective personal privacy protection legislation."

ACM US Technology Policy Committee
1701 Pennsylvania Ave NW, Suite 200
Washington, DC 20006

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

On behalf of USACM, thank you and the Subcommittee 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. Recognizing that these issues and their consequences extend far beyond any single online platform or channel, and that a robust understanding of relevant technology is essential to effectively legislating, the expert members of USACM and ACM – many of them true luminaries in computer science, engineering and associated disciplines – stand ready to assist your work in any way that we can.

Thank you for your consideration of both the technical and ethical recommendations detailed in the attached record statement, and for the Subcommittee's ongoing commitment to the public's protection. 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

CC: Hon. John Thune, Chairman
Senate Committee on Commerce, Science, and Transportation

Hon. Bill Nelson, Ranking Member
Senate Committee on Commerce, Science, and Transportation

Attachments

Statement for the Record of "Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks," June 19, 2018

* USACM's April 9 letter bore its prior name, "U.S. Public Policy Council," which changed to the above on July 1.

ACM US Technology Policy Committee
1701 Pennsylvania Ave NW, Suite 200
Washington, DC 20006

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

Before the
United States Senate
Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

STATEMENT OF THE ASSOCIATION FOR COMPUTING MACHINERY U.S. TECHNOLOGY POLICY COMMITTEE

Submitted for the record of
"Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks"

July 2, 2018

Before the
United States Senate
Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

STATEMENT OF THE ASSOCIATION FOR COMPUTING MACHINERY U.S. TECHNOLOGY POLICY COMMITTEE

Submitted for the record of
"Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks"

EXECUTIVE SUMMARY

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's U.S. Technology Policy Committee (USACM) is charged with providing policy and law makers throughout government with timely, substantive and apolitical input on computing technologies and the legal and social issues to which they give rise.

USACM commends the Committee and Subcommittee for delving deeply into the causes, consequences and implications of the Facebook/Cambridge Analytica data breaches and related failures to protect the information and privacy of millions and the integrity of democratic processes. This statement offers a synthesis of the circumstances of this series of choices and results. In addition, without endorsing any specific statutory proposal, it also makes a series of recommendations for how legislative and regulatory responses might be crafted to address the most serious technical and ethical issues raised by the Facebook/Cambridge Analytica matter, with broader applicability to all digital environments.

Fundamentally, USACM recommends that Congress craft and adopt comprehensive, risk-based privacy protections that achieve nine critical and distinct objectives. Those objectives, and USACM's conceptual recommendations for how regulators and enterprises can meet them, are:

1. **Limit collection and minimize retention of personal data**[1]
    - 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.

[1] The term "data" is used broadly throughout this statement to encompass personal information, patterns of individual behaviors, identifying imagery, and spatial presence.

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.

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*)

Given the significance and breadth of the privacy and ethical shortcomings at the core of the Cambridge Analytica matter, USACM believes that now is the time for Congress to act to protect the public interest and the integrity of the democratic process by adopting comprehensive and effective personal privacy protection legislation.

Before the
United States Senate
Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

STATEMENT OF THE
ASSOCIATION FOR COMPUTING MACHINERY
U.S. TECHNOLOGY POLICY COMMITTEE

Submitted for the record of
"Cambridge Analytica and Other Facebook Partners:
Examining Data Privacy Risks"

Although data[2] privacy issues create recurring challenges to a broad sector of industries, the social media context creates unique challenges. This is especially apparent in Facebook, the largest social media community in the world, the leading revenue generator in the industry, and the primary social media platform choice of Americans[3]. These challenges spring from:

1. **Scale** – Globally, there are approximately 2.2 billion Facebook, 1.5 billion YouTube, 813 million Instagram, and 330 million Twitter users of social media.[4] Among 325 million US adults, 68% use Facebook, 73% use YouTube, 35% use Instagram, and 24% use Twitter, and 60-75% of these are daily users.[5] This creates an enormous platform for data collection and third party usage.
2. **Influence** – The network structure of social media, where individuals are directly connected to friends and indirectly to friends of friends (and their friends), creates a highly effective platform for spreading influence through information and opinions. Services designed to build and reinforce healthy social connections can also be used to manipulate and influence opinion.
3. **Social context** – Compared to the individual and transactional nature of other online environments (e.g., banking, commerce, and health), social media is grounded in social interactions, relationships, and reputations. As such, decisions, behaviors, and consequences are rarely confined to the individual level.
4. **Assumptions of risks** – Connecting and sharing with friends are considered non-transactional and therefore appear to create less risk than online purchasing. Similarly, disclosures among trusted friends are considered less risky than public disclosures, and many users, regardless of their privacy settings, still consider their social media disclosures "among friends."
5. **Technical synergies** that reinforce effects create an environment that engenders problematic security and privacy practices. This includes platform architecture, data aggregation, micro-targeting algorithms, and application programming interfaces (APIs).

[2] The term "data" is used broadly throughout this statement to encompass personal information, patterns of individual behaviors, identifying imagery, and spatial presence.
[3] Smith, A., & Anderson, M. (2018, Mar 1). Social Media Use in 2018. *Pew Research Center.* http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/
[4] Statistica (2018). Social media: Statistics and facts. *Statistica: The statistics portal.* https://www.statista.com/topics/1164/social-networks/
[5] Smith, A., & Anderson, M. (2018, Mar 1). Social Media Use in 2018. *Pew Research Center.*

The unique circumstances of the Facebook-Cambridge Analytica data breach included consequences that extend beyond individual or social levels, to the disruption of national democratic processes. Data on US citizens was specifically harvested by agents outside of the US to develop predictive models and ads targeted at voter manipulation in the 2016 presidential election. This operation employed large-scale collection and sharing of datasets from the Facebook platform, under the guise of research. Derivative data were subsequently sold (at a price of $500,000) to a private data harvesting firm to develop profiles for targeted ad deployment. Assessments of the operation's effectiveness vary, but the very existence of the attempt to manipulate the public in this manner highlights the risks of social media data sharing.

The Cambridge Analytica incident illustrates the difficulties of monitoring and regulating data that is collected from one site (*Facebook*), analyzed at a second site (*Cambridge University*), and then sold to a third site (*Cambridge Analytica*) where it was used to influence our systems of government. Moreover, this situation was foreseeable, and specifically described in reports as early as 2010.[6] Furthermore, although Cambridge Analytica has closed its doors,[7] a new company has already been created (Data Propria) that includes employees from Cambridge Analytica and alleged access to the data collected from the Facebook community and its derivatives.[8]

In other words, election interference using social media channels and data mined from social media communities was predicted, has happened, and is continuing in current campaigns today – nationally and globally. This means that democracy in the United States remains vulnerable to the type of assault committed in 2016. The processes to inoculate voters against this influence or manipulation remain to be established. This should not be seen as a partisan activity but one to protect democracy from those who would do it harm.

This case and its breaches of data and trust challenge fundamental principles of privacy protection that have been enumerated in statements and laws over the years, including the *Fair Information Practice Principles* first codified in the US Privacy Act in 1974 [5 U.S.C. § 552a]. The case also raises questions about the ethical responsibilities of Facebook and other social media companies in their professional practice, as well as the design of platforms that advantage revenue over the protection of user privacy. We elaborate on these in the following sections.

[6] Electronic Privacy Information Center. (2010). e-Deceptive Campaign Practices (2010). http://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf, p. 25

[7] Ballhaus, R., & Gross, J. (2018, May 2). Cambridge Analytica Closing Operations Following Facebook Data Controversy. *Wall Street Journal*. https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140

[8] Horwitz, J. (2018, June 15). Trump 2020 working with ex-Cambridge Analytica staffers. *AP News.* https://apnews.com/96928216bdc341ada659447973a688e4

PRIVACY

Data capture mechanisms continue to evolve. Meanwhile, threat actors seek to exploit vulnerabilities to circumvent security and improperly access personal data (e.g., the 2015 OPM[9] and 2017 Equifax[10] data breaches). Given the number and magnitude of reported data breaches, the US, like the EU, is at a pivotal point, and must take a retrospective, holistic, and comprehensive view of data breaches. Policy makers should consider risk-based comprehensive privacy reform with broad privacy statements to maintain pace with technological advancements. Any new data privacy protections should aim to:

1. Limit collection and minimize retention of personal data

Numerous kinds of data collection within the Facebook platform exceed the scope expected by users and, in some cases, take place without the informed consent of the users. For example, data is collected about friends of friends (who were not given the opportunity to permit such data sharing), and through third-party apps. This data is then used for secondary or tertiary purposes without the knowledge or consent of users and sometimes, as in the case of Cambridge Analytica, in violation of third-party terms of agreement.

In addition, Facebook collects data on non-Facebook account holders, conducts off-platform tracking of users to support data security and platform interoperability, and accesses cookies to feed advertising delivery. Facebook also has data-sharing partnerships with more than 60 device makers, including Amazon, Apple, Microsoft, and Samsung,[11] as well as four Chinese electronics businesses, including one that has been identified as a national security threat.[12] The device-maker partnerships provide third party business associates with access to personal data of Facebook users and their friends, without explicit consent. Most of these collection activities are not transparent to users.

Recommendations:

- 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 all data collected or retained, regardless of how minimal or briefly held.

---

[9] Nakashima, E. (2014, Jul 9). Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say. *Washington Post*. https://www.washingtonpost.com/news/federaleye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authoritiessay/?utm_term=.305e75d6db3d

[10] Matthews, L. (2017, Sep 7). Equifax Data Breach Impacts 143 Million Americans. *Forbes*. https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-millionamericans/#5dd854a4356f

[11] Dance, G.J.X., Confessore, N., & LaForgia, M. (2018, June 3). Facebook Gave Device Makers Deep Access to Data on Users and Friends. N.Y. Times. https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html

[12] LaForgia, M. & Dance, G.J.X. (2018, June 5). Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence. N.Y. Times. https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html?smprod=nytcore-ipad&smid=nytcore-ipad-share

2. Clarify and simplify user consent processes and maximize user control of data

Addressing user consent in large-scale social media contexts is admittedly complicated, and current consent practices are generally ineffective. Specifically, consent in social media environments is overbroad (blanket consent for very nuanced uses of data), and users often consent even when the risks are high,[13] or because they fear a loss of functionality or missing out of social engagement.[14] Consent is also not transparent, because data is often used in multiple ways beyond the original collection purpose. Consent needs to be meaningful, granular, and an opt-in norm. These terms are described below:

- *Meaningful* consent acknowledges the complexity of privacy decision-making in social computing platforms and the difficulties of consent at scale. Consent in social media environments extends beyond individual decisions, and also considers relationships, organizational commitments and the social controls (laws, policies, and codes of conduct) in which an individual is embedded.[15]
- *Granular* consent means that disclosure decisions are specific and based upon details about the type of information, audience, communication channel, and intended use for the data. Such consent is transparent so that users understand how data will be used and who will see and use it. Granular consent should be applied to limit functionality loss when opting not to share certain data.
- Finally, a significant body of research indicates that *opt-in* defaults, where data sharing will not occur unless the user explicitly grants permission, are much more likely to align with user preferences than opt-out defaults.[16] [17] [18]

User consent policies must also address third-party data sharing and data provenance. In the Facebook/ Cambridge Analytica case, data was collected by a research-based "personality game."[19] Individuals may have read their privacy policy and been comfortable with data collection. But when their data is shared with third and fourth parties, data ownership and control of the data is often lost. Worse, in this case, friends of friends who did not provide consent for data collections, had their data released to a third party and manifest itself in unknown downstream locations. In general, U.S. laws do not provide protection for data that is reused and re-disclosed (except in sectoral law, e.g. HIPAA and GLBA). Thus, once information is leaked and in the possession of a third party, the person involved will not know who has the data, if it is correct or current, and has no control over it.

---

[13] Alessandro Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy, Jan./Feb.,* 26-29.

[14] Przybylski, A., Murayama, K., DeHaan, C., & Gladwell, V. (2013). Motivational, emotional and behavioural correlates of fear of missing out. *Computers in Human Behaviour, 29,* 1841-1848.

[15] Schwartz, P. M. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review, 52,* 1609-1612.

[16] Cranor, L. F., Guduru, P. & Arjula, M. (2006). User interfaces for privacy agents. *ACM Trans. Comput.-Human Interaction, 13,* 2 (June 2006), 135-178.

[17] Cranor, L. F. (2012). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications and High Technology Law, 10,* 273.

[18] McQuinn, A. (2017, October 6). The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules. https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules

[19] Kogan, A. (2018, June 19). *The Threat of Data Theft to American Consumers.* Testimony on behalf of USACM before the Senate Comm. on Commerce, Science and Transportation, S. Comm. on Consumer Protection, Product Safety, Insurance, and Data Security. Washington, DC. https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=484EFD3A-63F9-40BA-B212-12311F3DE7ED

Recommendations:

- Provide individuals with easily understood and centrally accessible consent options specific to the type, scope, and purpose of use to assure 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 informed consent.
- Encourage research into and the development of smart, automated privacy agents (e.g., P3P[20] was an early attempt) to infer privacy preferences, establish smart defaults[21], and scaffold decisions about consent and disclosure.

3. Simplify data sharing policies and assure transparency in data flows

Facebook has failed to provide clear and conspicuous notice of its data collection practices (e.g., friend of friend data capture, and off-platform data collection) and new uses of the data. Individuals are not given clear information regarding what data is being collected. Furthermore, Facebook has shared repurposed data with third parties without proper consent. Collection of data under the guise of social games (e.g., personality tests) obscures and violates transparency of data use. For example, apps that entice engagement but come attached with obscured ("back door") consent to allow data sharing, mask the true nature of platform engagement and data collection. Facebook also has device partnerships with over 60 device firms, and provides access to user data with these partners, including international firms with less secure data protection laws.[22]

Recommendations:

- Provide individuals, prior to data collection and creation, with clear and concise 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 and why it may be disclosed, and how they may access, modify, and delete their own 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.[23]

[20] Cranor, L. F., Guduru, P. & Arjula, M. (2006). User interfaces for privacy agents. *ACM Trans. Comput.-Human Interaction, 13*, 135-178.

[21] Knijnenburg, B.P. (2015). *A User-Tailored Approach to Privacy Decision Support.* PhD dissertation, University of California Irvine.

[22] Dance, G.I.X., Confessore, N., & LaForgia, M. (2018, June 3). *Facebook Gave Device Makers Deep Access to Data on Users and Friends,* N.Y. Times.

[23] Caine, K., Kisselburgh, L.G., & Lareau, L. (2011). Audience visualization influences online social network disclosure decisions. *Proc. of the 2011 Conference on Human Factors in Computing Systems,* 1663-1668.

4. Clearly define and disclose data ownership terms and attendant rights

It is critical to clarify differences in data types and how they affect the concept of ownership, and its underlying rights. During the April congressional hearings, Mark Zuckerberg provided numerous assurances that every Facebook user owns and controls their data, stating: "*This is the most important principle for Facebook. Every piece of content that you share on Facebook you own, and you have complete control over who sees it and how you share it*."[24]

But Facebook's "complete control" policy protects data that *users contribute* in postings and comments; the protections do not extend to data not explicitly provided by users, but instead derived from user behavior (i.e., *derivative data)*, such as liking behavior, friending patterns, metadata on content shared, and devices used. Furthermore, vast troves of data are collected from third party partners, app developers, and data brokers, who provide information about activities off Facebook, and are then aggregated with user-contributed data. Individuals do not have ownership, or complete control, over these data. (For an extensive list of data collected, see Mr. Zuckerberg's responses to the Senate Judiciary Committee.)[25]

In spite of its ongoing rhetoric of building social communities, by its own admission,[26] at its core Facebook is a platform to collect, generate, and commodify user data. Once engaged, individuals have relatively little control over how their data is used.

Recommendations:

- 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 the risk

Facebook relinquishes oversight after sharing data with third parties, and therefore does not audit or track uses beyond the original intent for which it was captured and shared. Nor is it alone in these practices. Considering the extensive and demonstrable risk presented by the accumulation of data (which is uniquely large-scale and detailed), little has been done to institute appropriate provisions to protect personal data. This should include risk assessments, processes to ensure that data is accessed according to Facebook policy, and proper auditing to track who is accessing what.

Recommendations:

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.

---

[24] *Facebook, Social Media Privacy, and The Use and Abuse of Data: Joint Hearing Before the* S. *Comm. On Commerce. Sci.,* & *Transp. and the* S. *Comm. on the Judiciary* (20 18) (statement of Mark Zuckerberg, Facebook).
[25] Facebook (2018, June). Responses to Judiciary Committee April 10, 2018 Hearing "*Facebook, Social Media Privacy, and the Use and Abuse of Data*" (p. 160-162).
[26] ibid (p. 155)

- Audit the access, use, and maintenance of personal data.
- Report data privacy breaches as quickly as possible.

6. Require clear, fair and responsible data access, retention, and disposal policies

The means by which users can expunge their Facebook data are not intuitive, and requesting that one's data be deleted may not actually result in expunged data. For example, it is difficult for users to remove underlying, internal data that is associated with their accounts, even when their account is deleted. Additionally, in the case of Cambridge Analytica, while Facebook assured users that data had been erased, they lacked an oversight process to ensure that data stored by the third and fourth parties (e.g., Cambridge University and Cambridge Analytica) was removed.

Recommendations:

- Establish clear policies with fixed, publicly stated retention periods and seek individuals' affirmative consent to retain their data for longer periods if desired by the collector.
- Reduce the risk of data loss by reducing the accessibility of data through de-identification, aggregation, encryption, and other methods.
- Implement an auditable process for validating the destruction of data when requested, including data provided to third, fourth, and other downstream parties.
- Store personal data only for as long as needed to serve the stated purpose for its initial collection.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including backup data and information shared with third parties.

7. Codify appropriate and meaningful oversight of third party developer platforms

Facebook's and others' application programming interface (API) developer platforms have been the source of many privacy breaches, allowed wide access to user data, and are subject to data use policies that often go unenforced. In 2017, for example, Facebook alone identified 370,000 apps that were in violation of its data use policy.[27] API platforms provide access to personal data to a variety of third parties, including app developers, advertisers, and researchers. However, the processes to regulate and audit anticipated use of personal data are not well enforced. Furthermore, by its own admission, the supplemental terms of service accompanying apps delivered in the Facebook platform are not reviewed.

This scenario has led to extensive background data scraping, and circumvented both user consent and data use oversight, and Cambridge Analytica was just one instance. API platform oversight must hold accountable all developers.

Recommendations:

- Publish clear guidelines for types of behavior that are acceptable and unacceptable for Facebook apps.

[27] Ibid (p. 217)

- Require oversight, review, and enforcement of policies regarding the types of apps and the uses of data that are allowed, with clear consequences for misuse.
- Ensure that the terms of service for all applications deployed are consistent with host data use policies.

8. Enable and support legitimate research when evaluated by qualified review boards

The rich user interactions and social dynamics of Facebook's and others' vast social networks represent a trove of opportunities for scientists interested in studying social dynamics and other related topics. Researchers are trained in, and ethically obligated to comply with, well-established regulatory frameworks that protect human participants in research studies. Facebook should both facilitate responsible research while working to ensure that the privacy of Facebook users is fully protected. [28] [29]

Recommendations:

- 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.

ETHICS

In addition to longstanding issues of privacy protection for user data in social media contexts, the Facebook/CA case raises many issues surrounding professional and organizational ethics. We suggest that Facebook, through repeated violations of privacy rights and insufficient concern for the consequences of such violations, has demonstrated a fundamental lack of ethical responsibility to its community and our larger society. Their actions, and their omissions, must be measured against appropriate ethical standards.

ACM, the world's longest-established and largest computing professional society, has a longstanding *Code of Ethics and Professional Conduct*[30] that holds computing professionals and organizations to standards of responsibility and ethical practice. Specifically, the first principle of the Code states that:

---

[28] Feamster, N. (2018, Apr 10). Freedom to Tinker: Is It Time for a Data Sharing Clearinghouse for Internet Researchers? *Center for Information Technology Policy,* Princeton University. https://freedom-to-tinker.com/2018/04/10/is-it-time-for-an-data-sharing-clearinghouse-for-internet-researchers/

[29] Smee, B. (2018, Apr 25). Facebook's data changes will hamper research and oversight, academics warn. *The Guardian.* https://www.theguardian.com/technology/2018/apr/25/facebooks-data-changes-will-hamper-research-and-oversight-academics-warn?CMP=share_btn_link

[30] ACM (2018). *Code of Ethics and Professional Conduct.* https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

> *"An essential aim of computing professionals is to minimize negative consequences of computing …and consider whether the results of their efforts… will be used in socially responsible ways."* (§1.1)

Fundamentally, Facebook (and other social media platforms) are designed to maximize user engagement and advertising revenue. Platforms for social engagement are based on trust and community and by their nature reduce concerns about privacy when one believes sharing is limited to friends. Users believe privacy policies protect sharing with friends.[31] [32] Yet, in spite of years of rhetoric to the contrary,[33] [34] the balance of care has minimized concerns of user privacy. While spokespersons for Facebook repeatedly have apologized for privacy breaches,[35] [36] [37] there has been no indication that Facebook will make fundamental changes to platform design to make privacy protections inherent rather than wholly dependent upon users.

In addition, Facebook's executives have repeatedly stated that they failed to recognize the potential misuse of data in their social community – a community of over 2 billion people, used by 68% of American adults. Ultimately, they abdicated what USACM and ACM's Code of Ethics consider their *heightened* responsibility to administer a platform that was deeply integrated into the fabric of 21st-century society, and neglected an appropriate standard of care for the members of its community and broader society.[38]

Furthermore, in the case of Cambridge Analytica, despite knowledge that data was being and had been misused, until the breach was publicized Facebook did not notify users and took few actions to alleviate the damage. Specifically, Facebook failed to identify and stop errant use of their API platform for nearly two years, and did not ensure the data was destroyed and no longer used. In this regard, they failed to abide by ethical standards regarding understanding and acknowledging the risks and consequences of systems, as well as legal standards of accountability to protect consumer privacy.[39]

---

[31] Wisniewski, P., Xu, H., Lipford, H.R., & Bello-Ogunu, E. (2015). Facebook Apps and Tagging: The Trade-off between Personal Privacy and Engaging with Friends. *J. of the Assoc. of Info Sci and Tech, 66* (9), 1883-96.

[32] Xu, H., Dinev, T., Smith, H.J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *J. of the Assoc. for Info Systems, 12*(12), 798– 824.

[33] Hoffmann, AL, Proferes, N., & Zimmer, M. (2016). "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society, 20*, 199-218.

[34] Zimmer, M. (2014, Feb 3). Mark Zuckerberg's theory of privacy. *Wash. Post.* http://wapo.st/1gHIpbl?tid=ss_mail&utm_term=.7137dd0e1d99.

[35] *Facebook, Social Media Privacy, and The Use and Abuse of Data.* Joint Hearing Before the S. Comm. on Commerce. Sci., & Transp. and the S. Comm. on the Judiciary, (20 18) (statement of Mark Zuckerberg, Facebook).

[36] Frenkel, S. (2018, May 22). Mark Zuckerberg to Apologize Again, This Time to European Parliament. *N.Y. Times.* https://www.nytimes.com/2018/05/22/technology/mark-zuckerberg-apologize-european-parliament.html

[37] Seetharaman, D. (2018, Mar 21). After Days of Silence, Facebook's Mark Zuckerberg Admits to 'Mistakes' with User Data. *Wall Street Journal*. https://www.wsj.com/articles/after-days-of-silence-mark-zuckerberg-to-publicly-address-facebooks-user-data-uproar-1521659989

[38] While this ethical standard was only recently included (in Section 3) of the Code of Ethics, 95% of surveyed ACM members responding agree it is important.

[39] Federal Trade Commission (2011, Nov 29). Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises. https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

At the same time, there are significant unresolved issues regarding ethical research practices in social media contexts, in both federally and privately funded venues. This includes discerning whether data is considered private or public, the challenge of garnering consent in large-scale contexts, and the ethical responsibility to inform users (either before, or by debrief after) experimental manipulation is conducted. For example, there were two published research studies conducted by Facebook involving political[40] and emotional[41] manipulation that raised significant questions in the research community about ethical research standards in social media environments.

Significantly, the use of harvested data to psychologically manipulate behavior extends beyond the generation of revenue streams to support a free community of social networking,[42] and should include careful oversight. Furthermore, given the findings of research demonstrating that political manipulation in the Facebook platform can be accomplished,[43] [44] the organization had an ethical duty to review and screen targeted ads that were designed to manipulate political opinion, and clearly failed to do this in 2016.

Codes of ethical practice exist to guide the developer in the design, development, and management of systems, and to recognize the human as well as system consequences of design failure. Computer professionals and organizations must adhere to these broadly accepted norms and ethical codes:

1. **Avoid harm to others**, where harm includes negative consequences or the undesirable loss of information or property (ACM Code § 1.2): The many cases of data breaches and disclosure of personal data within Facebook and other social media platforms, as well as the use of Facebook for political manipulation of voters, has undeniably caused harm to global citizens.
2. **Respect privacy** (ACM Code § 1.6): As numerated earlier, there are fundamental, longstanding principles of privacy protection that have been ignored both in practice as well as in system design.
3. **Evaluate the possible risks** of the systems they develop (ACM Code § 2.5): By their own admission,[45] Facebook executives failed to recognize, understand, and assess the risks inherent in any platform that handles information about people. Given the vast size and influence of the Facebook platform, this was fundamentally negligent.
4. **Ensure that the public good is a central concern** (ACM Code § 3.1): With 69% of Americans using social media, and most of them on a daily basis, these are effectively public utilities with commensurate obligations to ensure the public good.

---

[40] Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature*, *489*(7415).

[41] Kramer, A.D.I., Guillory, J.E., & Hancock, J.T. (2014). Emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788-8790.

[42] Woodruff, J. (2018, Apr 5). Facebook 'made big mistakes' on protecting user data. *PBS Newshour.* https://www.pbs.org/newshour/show/sheryl-sandberg-facebook-made-big-mistakes-on-protecting-user-data

[43] Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature*, *489*(7415).

[44] Electronic Privacy Information Center. (2010). e-Deceptive Campaign Practices (2010). http://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf, p. 25

[45] *Facebook, Social Media Privacy, and The Use and Abuse of Data: Joint Hearing Before the* S. *Comm. On Commerce. Sci.,* & *Transp. and the* S. *Comm. on the Judiciary* (20 18) (statement of Mark Zuckerberg, Facebook).

5. **Provide responsible stewardship of systems embedded in society** (ACM Code §3.7)**:** The ACM Code recently was revised to add: **"**When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems."

CONCLUSION

US citizens enjoy an expectation of privacy when talking on standard landline telephones. Eavesdropping on another's call is prohibited by the Wiretap Act [18 U.S. Code § 2511]. Similarly, US citizens have an expectation of privacy when mailing a letter, as codified by 18 U.S. Code § 1708. However, legislation has not kept pace with technological advancements. For example, these same protections for mail and telephone do not extend to electronic communications, such as email, twitter feeds, or social media posts. Instead, data from these channels are captured, aggregated, correlated, shared, and sold. Processes like deep packet inspection, web beacons, and parsing email content seem equally intrusive. If you call your closest relative and share that you have the flu, that conversation is protected. However, if you email those same disclosures, that communication is subject to being captured, shared, and aggregated.

Certainly, businesses have legitimate reasons to collect certain kinds of data. When making an online purchase, specific information is required (such as item, cost, payment, and location) to deliver the merchandise. Consumers see value in providing these details to fulfill a transaction. However, if the purchased merchandise was for an adult product, one might be troubled to know the merchant sold those details to a background screening company, who included that information when you later applied for a new job. Clearly some data needs to be collected. At issue are: what data to collect, how long is the data retained, is it accurate and protected, what other datasets are combined with it, and with whom is this data shared.

In summary, data collection, sharing, and management practices in the US have gone largely unregulated. Facebook illustrates that organizations will continue to evolve their business models, sometimes to the detriment of consumers' security and privacy. The issues are exacerbated by the constant invention of new data collection channels (e.g., smart speakers, wearable fitness trackers, smart appliances). The type and amount of data being captured is unprecedented, as is the velocity of which it is shared. The ability to cross-reference seemingly disparate data to draw conclusions is alarming. Large data stores can be monetized quickly and the raw materials to create these products are not consumed when they are sold, so they can be repackaged in perpetuity.

As technological innovation continues its exponential growth, ethical platform design and professional practice and broad scalable legislation and oversight are needed. Policy and laws that were once adequate, like the Wiretap Act, do not account for the complexities of today's socio-technical systems. Businesses today have proven unable to self-police, and so legislative and regulatory action that protects consumer privacy without materially limiting innovation is essential.

Specifically, protections are needed that limit data collection, require granular consent, transparently articulate information collection and retention, prohibit reuse/re-disclosure without informed consent, introduce expiration dates for datasets that deteriorate over time, consider the ethical consequences, introduce constructs to validate that consumer safeguards are effective, and enforce these protections.

Finally, a social media platform like Facebook is a single channel. But the broader picture indicates that technological advancements will continue to outpace legislation and consumers' ability to understand the ramifications of the types and amount of data being captured. Recognizing this, niche legislation (e.g., to address only social media) will not adequately protect consumers and will be constantly chasing emerging technological advancements. Further, given the monetary incentives, businesses will continue to find loopholes, or will alter their business model to stay ahead of legislation. Even if businesses are somehow enticed to be better data stewards, the number of publicized data breaches suggests the data will continue to leak into the wild.

Given the significance and breadth of these privacy and ethical shortcomings, USACM believes that now is the time for Congress to act to protect the public interest and the integrity of the democratic process by adopting comprehensive and effective personal privacy protection legislation.*

Respectfully submitted,

Stuart Shapiro, Chair

acm U.S. Technology Policy Committee

July 2, 2018

---

* This document is a product of the ACM US Technology Policy Committee. In consultation with the colleagues noted below affiliated with ACM's Europe Technology Policy Committee (EUACM), it was prepared by the following USACM members:

Principal Authors:
Dr. Lorraine Kisselburgh, Purdue University (Chair, USACM Ethics Working Group)
Brian Dean, Secureworks (Chair, USACM Privacy Subcommittee)

Contributors:
Dr. Flo Appel, Saint Xavier University
Lillie Coney, Independent Policy Expert
Dr. Nick Feamster, Princeton University
Dr. Fabrizio Gagliardi, Barcelona Supercomputing Center (Chair, EUACM)
Dr. Simson Garfinkel, US Census Bureau (Co-Chair, USACM AI & Algorithmic Transparency Committee)
Barb Helfer, Immersion Corporation
Andy Oram, O'Reilly Media
Marc Rotenberg, J.D., Electronic Privacy Information Center, Georgetown University
Dr. George Roussos, University of London
Dr. Stuart Shapiro, MITRE Corporation (Chair, USACM)

NOTE: Non-USACM affiliations noted above are provided solely for author identification purposes. They do not signify or imply the views or endorsement of any named entity other than USACM.

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.

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.

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