From: Adam Eisgrau <eisgrau@hq.acm.org>
Sent: Thursday, October 24, 2019 1:37 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments of ACM US Technology Policy Committee

Ms. MacFarland:

On behalf of the U.S. Technology Policy Committee of the Association for Computing Machinery, I am pleased to timely submit the attached Comments on NIST's Preliminary Draft Privacy Framework noticed for public comment on September 9, 2019 (84 FR 47255, Document 2019-19315). Please contact me directly should you have any questions regarding the Committee's comments, or if ACM's expert members can further assist NIST's future work on the Framework in any way. Thank you.

Adam Eisgrau

Director of Global Policy and Public Affairs

ACM -- Association for Computing Machinery

+1.202.580.6555

www.acm.org

October 24, 2019

Submitted Electronically

Kevin A. Kimball, Chief of Staff
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: ACM U.S. Technology Policy Committee Comments on
September 6 Preliminary Draft NIST Privacy Framework

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 safeguards are needed to protect the personal privacy of all U.S. citizens. We thus applaud the National Institute of Standards and Technology ("NIST") for its extensive and transparent process for development of the Preliminary Draft Privacy Framework ("Framework"),[1] and for the thoroughness of the Framework itself. Most fundamentally, we also appreciate and endorse the Framework's flexible, risk-based approach, which crucially will allow it to "scale" for organizations of widely varied size and complexity.[2]

In response to NIST's recent Request for Comment, the Committee is pleased to again contribute[3] to the ongoing process of strengthening and refining the Framework. To that end, the Committee offers the following observations and recommendations:

[1] "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management" (Sept. 6, 2019)

[2] See, however, discussion of Section 3.4, below.

[3] The Committee initially provided feedback in this proceeding in its *Comments to National Institute of Standards and Technology on Developing a Privacy Framework* of January 14, 2019. It was also represented at NIST's third workshop on the Framework in Atlanta, Georgia by Lorraine Kisselburgh of Purdue University and Chair of ACM's global Technology Policy Council. The Committee's commitment to and engagement in the issues addressed by the Framework are longstanding. See, *e.g.*, its March 2018 *Statement on the Importance of Preserving Personal Privacy* and 2015 *Comments to the National Institute of Standards and Technology on Privacy Risk Management*.

- The NIST Privacy Framework's core architecture is in general a sound and effective means of conceptualizing and visualizing the multiplicity of objectives and modalities inherent in NIST's Framework effort. Further, the inclusion of "Control" among the specific functions integral to a successful privacy policy is particularly constructive. The Committee is concerned, however, that additional privacy protections must be included among the objectives directly addressed and sought within the "Disassociated Processing" Category of the Control function (CT.DP-P) as illustrated in Table 1.[4] Specifically, as emphasized in the Committee's own *Statement on the Importance of Preserving Personal Privacy* of March 2018, the concept of "permissible use" must be woven into both the broad concept of Control and its granular expression throughout the Framework.

  For example, with reference to the Subcategory detail associated with "data processing" within the Category of Disassociated Processing (CT.DP-P6), the Committee believes it insufficient to limit data collected only to information "necessary…to meet mission/ business objectives." Rather, in addition, the explicit and informed consent of an individual must be a prerequisite to any reuse or redisclosure of the data for any purpose beyond the one for which it was collected in the first instance. No other use should, absent real consent, be permissible.[5]

- In Section 3.4, we concur that attention in the Framework to the System Development Life Cycle ("SDLC") is imperative, but are concerned that the draft discussion is not sufficiently nuanced, risking negative effect, in two respects:

  - First, while it notes that the evolution of systems is an issue of which to be cognizant, the Framework does not adequately acknowledge that for larger enterprises most systems spend many more years in "evolution mode" than in development. We thus recommend that, to also be germane to such enterprises, the next iteration of the Framework expressly consider and address in detail the consequences of evolution, which will only become more profound over time as marketplace trends toward "self-service" evolution (the organic extension of software applications by businesses) accelerate.

  - Second, the Framework appears to explicitly consider only traditional "waterfall" SDLC processes. Many alternative forms exist, however, and application of the Framework to them may prove challenging. We recommend that this be addressed, or at least acknowledged, in future drafts of the Framework.

- In Section 3.4, we also urge NIST in future versions of the Framework to explicitly recognize that its application to the SDLC is a matter of both process and *infrastructure*, which must

[4] Framework, p. 20.

[5] The Committee notes that this issue is addressed to an extent in connection with Framework Subcategories CT.PO-P1 and P3, but believes on balance that the level of clarity and emphasis on this point recommended above is essential.

deliberately be configured to support application of the Framework. Such prioritization will require management's systematized attention and commitment of resources, both human and financial. We urge NIST to make this interdependency explicit in future versions of the Framework and to stress its centrality to successful application of the Framework in practice.

- With respect to the "Privacy Engineering" Objectives noted in Table 3 of the Framework:[6]
    - Concerning "Predictability":
        - Specifically address *fairness*. With the foreseeable exponential expansion of automated decision-making technology, the Framework should make clear that an individual generally[7] should be provided with sufficient information in non-technical terms to understand the factors assessed by an automated system or algorithm in making an adverse determination or decision about that individual.[8]
        - Broaden and deepen the Framework's treatment of *transparency*. The Committee appreciates the intent of the Framework's "Communicate" function ("CM-P") and the utility of the details provided in the associated Category, particularly Subcategory CM.PP-P1. We believe, however, that it also should state that individuals must be provided 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, correct and expunge their own data; and the process by which the holder of the data may be contacted with complaints or requests. The exponential proliferation of Internet of Things connectivity to be anticipated makes this essential.
    - Concerning "Manageability":
        - Specifically address *limited collection*. A hallmark of any acceptable privacy policy must be that personal data is collected and retained *only* when strictly necessary either to provide the service or product to which the data relates, or to achieve a legitimate societal objective.
        - The Framework's discussion of its Govern function ("GV-P") is admirably extensive. We recommend, however, that it be expanded to also note key elements and objectives of an effective data administration *enforcement* regime.

[6] Framework, p. 35.

[7] Limited exception to this precept may be necessary or desirable when knowledge of such factors would permit "gaming" of the very system or process in which the individual has opted to participate, *e.g.*, online dating.

[8] The Committee notes that "fairness" may be viewed as a specific aspect of predictability addressed at Subcategory ID.RA-P2 of the Framework. We believe, however, that fairness is a more complex matter than that discussion of bias alone can adequately address and thus encourage NIST to consider multiple aspects of fairness in greater depth in future Framework drafts.

ACM's U.S. Technology Policy Committee appreciates the opportunity to comment on NIST's Preliminary Draft Privacy Framework. We look forward to future stages of the Framework drafting and comment process and are available should you have questions concerning, or would like additional information about, any of the issues raised in these Comments.[9] In that event, please contact Adam Eisgrau, ACM's Director of Global Policy and Public Affairs at 202-580-6555 or acmpo@acm.org.

Sincerely,

James A. Hendler
Chair

[9] This submission reflects the primary input of the ACM U.S. Technology Policy Committee Privacy Subcommittee Chair Brian Dean and Subcommittee members Paul Hyland, Joshua Kroll, Arnon Rosenthal and Stuart Shapiro.