
May 26, 2020

# STATEMENT ON SECURITY AND PRIVACY PRINCIPLES FOR VIRTUAL MEETINGS

The COVID-19 pandemic has rapidly driven individuals and communities worldwide to interact over the Internet in new ways. Consequently, and with a speed rarely seen, virtual conferencing platforms have been pressed into service for new uses by large categories of users to facilitate previously non-virtual aspects of everyday life. These diverse interactions include, for example, religious services, birthday parties, departmental meetings, weddings, medical appointments, psychotherapist sessions, and high-level government consultations.

This new reliance on virtual conferencing platforms and technology has exposed significant challenges to assuring their privacy and security:

- Many such platforms incorporate limited security and privacy controls. While such tools might have been sufficient when needed only for occasional public-facing events, they are insufficient for use at enormous scale and in more sensitive applications.

- Many new videoconferencing users are not trained in using these technologies or in underlying principles of online security and privacy.

- In most cases, adoption is taking place quickly and out of necessity, without adequate opportunities to consider such important issues as security training, threats to privacy, impacts on vulnerable communities, accessibility, or applicable laws such as the European Union's General Data Protection Regulation (GDPR) and the US Family Educational Rights and Privacy Act (FERPA).

The U.S. Technology Policy Committee (USTPC) of the Association for Computing Machinery (ACM) is committed to providing technical information to policymakers, all interested communities, and the public in the service of sound public policy formation, and safe software design and deployment. Consistent with ACM's Code of Ethics and Professional Conduct, USTPC urges the broad adoption of the following security and privacy principles for virtual conferencing platform technology.*

---

* For more on these principles and the rationale for their adoption, *see* *Virtual Conferences: A Guide to Best Practices*, ACM Presidential Task Force on What Conferences Can Do to Replace Face-to-Face Meetings (April 13, 2020) and *Security and Privacy Principles for Virtual Meetings*, a white paper by USTPC members Simson Garfinkel, Jeanna Matthews, Andy Oram, Patrick Traynor and Alec Yasinsac.


# ASSOCIATION FOR COMPUTING MACHINERY
# U.S. TECHNOLOGY POLICY COMMITTEE
# SECURITY AND PRIVACY PRINCIPLES FOR VIRTUAL MEETINGS

## Security

S1. Platforms should be constructed initially, and evaluated and refined throughout their life cycles, to minimize or prevent both intentional and inadvertent disruption.

S2. Platform architecture should incorporate end-to-end encryption of meeting data, both in transit and in archival form.

S3. Recordings should be stored in a protected location. Default options for recordings should include encryption, sharing only with designated individuals, and a limited retention period.

S4. Platform design should permit hosts and other administrators to:

a) specify access control on several levels, per session, and per participant, as well as to provide useful default settings;

b) determine the level of trust among participants (rather than the software making assumptions of trust based on shared characteristics such as a common domain name);

c) make detailed access control choices for a meeting once and then easily reuse them as a template for other similar meetings;

d) generate fresh contact information for each authorized participant without forcing a reset of all access controls for each meeting;

e) employ robust vetting functions to control meeting access; and

f) designate and enable additional individuals to assist with discrete conference functions, including specifically attendee vetting and disruptive attendee management.

## Privacy

P1. Platform users should be transparently and completely able to determine:

a) whether the meeting is being recorded, by means of a clear and accessible indicator;

b) what information about them is visible to other conference participants; and

c) who is hosting the conference and what controls the host is applying to the meeting.

ACM U.S. Technology Policy Committee
1701 Pennsylvania Avenue, N.W. #200
Washington, D.C. 20006

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

P2. Platforms should enable users with:

a) opt-in or, at minimum, opt-out controls for attendees;

b) support for post-meeting editing (including "undo" functionality); and

c) anonymous or pseudonymous participation options, where appropriate.

P3. Platforms should not:

a) collect user information not needed to provide the platform's service; and

b) provide a user's information to third parties unless individual users make a clearly presented choice to opt-in to such data sharing.

P4. Hosts should designate, and attendees should be encouraged to follow, a code of conduct for the meeting which includes:

a) notification by participants to other attendees when non-participants nearby may be able to hear or see the meeting; and

b) limits on capturing and/or sharing screenshots and other meeting information.

May 26, 2020

ACM U.S. Technology Policy Committee
1701 Pennsylvania Avenue, N.W. #200
Washington, D.C. 20006

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