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

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

POLICY STATEMENT ON MANDATORY ENGINEERED LAW ENFORCEMENT ACCESS TO INFORMATION INFRASTRUCTURE AND DEVICES

The power and prevalence of systems and devices that encrypt data have increased dramatically in recent years, affording the users of such systems and devices virtually complete control over access to encrypted data. In response, some in Congress, the Executive Branch and the law enforcement community have called for the designers and providers of such robust encryption technology to ensure data are accessible to law enforcement.

Specifically, it has been suggested that the designers of such encryption systems, and the commercial and other institutions that employ them, should create or be legally compelled to create extraordinary means of access to them that would override or circumvent passwords and other user controls. Such engineered "backdoors" and other means of extraordinary access would be employed as judicially authorized under appropriate circumstances to permit law enforcement access to information on communications networks, or stored in personal and commercial digital devices.

USACM is committed to providing technical information to policymakers, all interested communities and the public in the service of sound public policy formation on this important matter. The points below represent USACM's collective view of current scientific understandings and will be revisited and/or republished as significant technical developments warrant. With respect to mandated extraordinary access to user-controlled encryption systems, USACM finds:

- No practical or theoretical engineering solutions of which we are aware have emerged to date that would provide law enforcement access to encrypted information solely under the control of the user of a robust encryption system.
- All presently known means of engineering extraordinary access to encrypted user information necessarily would introduce security vulnerabilities that would expose the involved systems to attack by malicious or otherwise extra-legal actors.
- Any proposed future technological means of affording extraordinary access to encrypted systems should be subjected to rigorous analysis and detailed Congressional consideration of all risks and benefits, including the potential access such a mechanism would provide to entities beyond the US, before being implemented.
- Effective judicial and congressional oversight of any extraordinary access techniques ultimately employed will require the mandated use of state-of-the-art audit trail and other tamper-resistant verification technologies.
- Additional research into means of providing extraordinary access to encryption systems for law enforcement purposes, and the risks and benefits potentially associated with them, is needed to make informed policy on this topic. A public process to develop and evaluate such technology would be most appropriate to materially advance knowledge in this area.

April 12, 2018

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

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