An Open Letter from US Researchers in Cryptography and Information Security

Media reports since last June have revealed that the US government conducts domestic and international surveillance on a massive scale, that it engages in deliberate and covert weakening of Internet security standards, and that it pressures US technology companies to deploy backdoors and other data-collection features. As leading members of the US cryptography and information-security research communities, we deplore these practices and urge that they be changed.

Indiscriminate collection, storage, and processing of unprecedented amounts of personal information chill free speech and invite many types of abuse, ranging from mission creep to identity theft. These are not hypothetical problems: they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-center links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities.

The value of society-wide surveillance in preventing terrorism is unclear, but the threat that such surveillance poses to privacy, democracy, and the US technology sector is readily apparent. Because transparency and public consent are at the core of our democracy, we call upon the US government to subject all mass-surveillance activities to public scrutiny and to resist the deployment of mass-surveillance programs in advance of sound technical and social controls. In finding a way forward, the five principles promulgated at http://reformgovernmentsurveillance.com/ provide a good starting point.

The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users. Every country, including our own, must give intelligence and law-enforcement authorities the means to pursue terrorists and criminals, but we can do so without fundamentally undermining the security that enables commerce, entertainment, personal communication, and other aspects of 21st-century life. We urge the US government to reject society-wide surveillance and the subversion of security technology, to adopt state-of-the-art, privacy-preserving technology, and to ensure that new policies, guided by enunciated principles, support human rights, trustworthy commerce, and technical innovation.

Martín Abadi  
Professor Emeritus, University of California, Santa Cruz

Hal Abelson  
Professor, Massachusetts Institute of Technology

Alessandro Acquisti  
Associate Professor, Carnegie Mellon University

Boaz Barak  
Editorial-board member, Journal of the ACM

Mihir Bellare  
Professor, University of California, San Diego

Steven Bellovin  
Professor, Columbia University

Matt Blaze  
Associate Professor, University of Pennsylvania

L. Jean Camp  
Professor, Indiana University

Ran Canetti  
Professor, Boston University and Tel Aviv University
This letter can be found at: http://MassSurveillance.info

Institutional affiliations for identification purposes only. This letter represents the views of the signatories, not necessarily those of their employers or other organizations with which they are affiliated.

1 The Association for Computing Machinery (ACM) is the premier organization of computing professionals.
2 CRYPTO is an annual research conference sponsored by the International Association for Cryptologic Research.