

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.

<i>Martín Abadi</i>	Professor Emeritus, University of California, Santa Cruz
<i>Hal Abelson</i>	Professor, Massachusetts Institute of Technology
<i>Alessandro Acquisti</i>	Associate Professor, Carnegie Mellon University
<i>Boaz Barak</i>	Editorial-board member, <i>Journal of the ACM</i> ¹
<i>Mihir Bellare</i>	Professor, University of California, San Diego
<i>Steven Bellovin</i>	Professor, Columbia University
<i>Matt Blaze</i>	Associate Professor, University of Pennsylvania
<i>L. Jean Camp</i>	Professor, Indiana University
<i>Ran Canetti</i>	Professor, Boston University and Tel Aviv University

<i>Lorrie Faith Cranor</i>	Associate Professor, Carnegie Mellon University
<i>Cynthia Dwork</i>	Member, US National Academy of Engineering
<i>Joan Feigenbaum</i>	Professor, Yale University
<i>Edward Felten</i>	Professor, Princeton University
<i>Niels Ferguson</i>	Author, <i>Cryptography Engineering: Design Principles and Practical Applications</i>
<i>Michael Fischer</i>	Professor, Yale University
<i>Bryan Ford</i>	Assistant Professor, Yale University
<i>Matthew Franklin</i>	Professor, University of California, Davis
<i>Juan Garay</i>	Program Committee Co-Chair, CRYPTO ² 2014
<i>Matthew Green</i>	Assistant Research Professor, Johns Hopkins University
<i>Shai Halevi</i>	Director, International Association for Cryptologic Research
<i>Somesh Jha</i>	Professor, University of Wisconsin – Madison
<i>Ari Juels</i>	Program Committee Co-Chair, 2013 ACM Cloud-Computing Security Workshop ¹
<i>M. Frans Kaashoek</i>	Professor, Massachusetts Institute of Technology
<i>Hugo Krawczyk</i>	Fellow, International Association for Cryptologic Research
<i>Susan Landau</i>	Author, <i>Surveillance or Security? The Risks Posed by New Wiretapping Technologies</i>
<i>Wenke Lee</i>	Professor, Georgia Institute of Technology
<i>Anna Lysyanskaya</i>	Professor, Brown University
<i>Tal Malkin</i>	Associate Professor, Columbia University
<i>David Mazières</i>	Associate Professor, Stanford University
<i>Kevin McCurley</i>	Fellow, International Association for Cryptologic Research
<i>Patrick McDaniel</i>	Professor, The Pennsylvania State University
<i>Daniele Micciancio</i>	Professor, University of California, San Diego
<i>Andrew Myers</i>	Professor, Cornell University
<i>Rafael Pass</i>	Associate Professor, Cornell University
<i>Vern Paxson</i>	Professor, University of California, Berkeley
<i>Jon Peňa</i>	Professor, Carnegie Mellon University
<i>Thomas Ristenpart</i>	Assistant Professor, University of Wisconsin – Madison
<i>Ronald Rivest</i>	Professor, Massachusetts Institute of Technology
<i>Phillip Rogaway</i>	Professor, University of California, Davis
<i>Greg Rose</i>	Officer, International Association for Cryptologic Research
<i>Amit Sahai</i>	Professor, University of California, Los Angeles
<i>Bruce Schneier</i>	Fellow, Berkman Center for Internet and Society, Harvard Law School
<i>Hovav Shacham</i>	Associate Professor, University of California, San Diego
<i>Abhi Shelat</i>	Associate Professor, University of Virginia
<i>Thomas Shrimpton</i>	Associate Professor, Portland State University
<i>Avi Silberschatz</i>	Professor, Yale University
<i>Adam Smith</i>	Associate Professor, The Pennsylvania State University
<i>Dawn Song</i>	Associate Professor, University of California, Berkeley
<i>Gene Tsudik</i>	Professor, University of California, Irvine
<i>Salil Vadhan</i>	Professor, Harvard University
<i>Rebecca Wright</i>	Professor, Rutgers University
<i>Moti Yung</i>	Fellow, Association for Computing Machinery ¹
<i>Nickolai Zeldovich</i>	Associate Professor, Massachusetts Institute of Technology

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.