pdf version

An Open Letter from US Researchers in Cryptography and Information Security

January 24, 2014

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*[1]
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
	Professor, Boston University

Ran Canetti	and Tel Aviv University
Lorrie Faith Cranor	Associate Professor, Carnegie Mellon University
Cynthia Dwork	Member, US National Academy of Engineering
Joan Feigenbaum	Professor, Yale University
Edward Felten	Professor, Princeton University
Niels Ferguson	Author, *Cryptography Engineering: Design Principles and Practical Applications*
Michael Fischer	Professor, Yale University
Bryan Ford	Assistant Professor, Yale University
Matthew Franklin	Professor, University of California, Davis
Juan Garay	Program Committee Co-Chair, CRYPTO[2] 2014
Matthew Green	Assistant Research Professor, Johns Hopkins University
Shai Halevi	Director, International Association for Cryptologic Research
Somesh Jha	Professor, University of Wisconsin – Madison
Ari Juels	Program Committee Co-Chair, 2013 ACM Cloud-Computing Security Workshop[1]
M. Frans Kaashoek	Professor, Massachusetts Institute of Technology
Hugo Krawczyk	Fellow, International Association for Cryptologic Research
Susan Landau	Author, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*
Wenke Lee	Professor, Georgia Institute of Technology
Anna Lysyanskaya	Professor, Brown University
Tal Malkin	Associate Professor, Columbia University
David	Associate Professor, Stanford

Mazières	University
Kevin McCurley	Fellow, International Association for Cryptologic Research
Patrick McDaniel	Professor, The Pennsylvania State University
Daniele Micciancio	Professor, University of California, San Diego
Andrew Myers	Professor, Cornell University
Rafael Pass	Associate Professor, Cornell University
Vern Paxson	Professor, University of California, Berkeley
Jon Peha	Professor, Carnegie Mellon University
Thomas Ristenpart	Assistant Professor, University of Wisconsin – Madison
Ronald Rivest	Professor, Massachusetts Institute of Technology
Phillip Rogaway	Professor, University of California, Davis
Greg Rose	Officer, International Association for Cryptologic Research
Amit Sahai	Professor, University of California, Los Angeles
Bruce Schneier	Fellow, Berkman Center for Internet and Society, Harvard Law School
Hovav Shacham	Associate Professor, University of California, San Diego
Abhi Shelat	Associate Professor, University of Virginia
Thomas Shrimpton	Associate Professor, Portland State University
Avi Silberschatz	Professor, Yale University
Adam Smith	Associate Professor, The Pennsylvania State University
Dawn Song	Associate Professor, University of California, Berkeley
Gene Tsudik	Professor, University of California, Irvine
Salil Vadhan	Professor, Harvard University

Rebecca Wright	Professor, Rutgers University
Moti Yung	Fellow, Association for Computing Machinery[1]
Nickolai Zeldovich	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.