

President Barack Obama  
The White House  
1600 Pennsylvania Avenue NW  
Washington, DC 20500

May 19, 2015

Dear President Obama,

We the undersigned represent a wide variety of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online, as well as technology companies, trade associations, and security and policy experts. We are writing today to respond to recent statements by some Administration officials regarding the deployment of strong encryption technology in the devices and services offered by the U.S. technology industry. Those officials have suggested that American companies should refrain from providing any products that are secured by encryption, unless those companies also weaken their security in order to maintain the capability to decrypt their customers' data at the government's request. Some officials have gone so far as to suggest that Congress should act to ban such products or mandate such capabilities.

**We urge you to reject any proposal that U.S. companies deliberately weaken the security of their products. We request that the White House instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology. Such policies will in turn help to promote and protect cybersecurity, economic growth, and human rights, both here and abroad.**

Strong encryption is the cornerstone of the modern information economy's security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, repressive governments trying to stifle dissent, or foreign intelligence agencies trying to compromise our and our allies' most sensitive national security secrets.

Encryption thereby protects us from innumerable criminal and national security threats. This protection would be undermined by the mandatory insertion of any new vulnerabilities into encrypted devices and services. Whether you call them "front doors" or "back doors", introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government's own experts.

In addition to undermining cybersecurity, any kind of vulnerability mandate would also seriously undermine our economic security. U.S. companies are already struggling to maintain international trust in the wake of revelations about the National Security Agency's surveillance programs. Introducing mandatory vulnerabilities into American products would further push many customers—be they domestic or international,

individual or institutional—to turn away from those compromised products and services. Instead, they—and many of the bad actors whose behavior the government is hoping to impact—will simply rely on encrypted offerings from foreign providers, or avail themselves of the wide range of free and open source encryption products that are easily available online.

More than undermining every American's cybersecurity and the nation's economic security, introducing new vulnerabilities to weaken encrypted products in the U.S. would also undermine human rights and information security around the globe. If American companies maintain the ability to unlock their customers' data and devices on request, governments other than the United States will demand the same access, and will also be emboldened to demand the same capability from their native companies. The U.S. government, having made the same demands, will have little room to object. The result will be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes. That's not a future that the American people or the people of the world deserve.

The Administration faces a critical choice: will it adopt policies that foster a global digital ecosystem that is more secure, or less? That choice may well define the future of the Internet in the 21<sup>st</sup> century. When faced with a similar choice at the end of the last century, during the so-called "Crypto Wars", U.S. policymakers weighed many of the same concerns and arguments that have been raised in the current debate, and correctly concluded that the serious costs of undermining encryption technology outweighed the purported benefits. So too did the President's Review Group on Intelligence and Communications Technologies, who unanimously recommended in their December 2013 report that the US Government should "(1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

We urge the Administration to follow the Review Group's recommendation and adopt policies that promote rather than undermine the widespread adoption of strong encryption technologies, and by doing so help lead the way to a more secure, prosperous, and rights-respecting future for America and for the world.

Thank you,

**Civil Society Organizations**

Access

Advocacy for Principled Action in Government

American-Arab Anti-Discrimination Committee (ADC)

American Civil Liberties Union

American Library Association

Benetech

Bill of Rights Defense Committee

Center for Democracy & Technology  
Committee to Protect Journalists  
The Constitution Project  
Constitutional Alliance  
Council on American-Islamic Relations  
Demand Progress  
Defending Dissent Foundation  
DownsizeDC.org, Inc.  
Electronic Frontier Foundation  
Electronic Privacy Information Center (EPIC)  
Engine  
Fight for the Future  
Free Press  
Free Software Foundation  
Freedom of the Press Foundation  
GNOME Foundation  
Human Rights Watch  
The Media Consortium  
New America's Open Technology Institute  
Niskanen Center  
Open Source Initiative  
PEN American Center  
Project Censored/Media Freedom Foundation  
R Street  
Reporters Committee for Freedom of the Press  
TechFreedom  
The Tor Project  
U.S. Public Policy Council of Association for Computing Machinery  
World Privacy Forum  
X-Lab

### **Companies & Trade Associations**

ACT | The App Association  
Adobe  
Apple Inc.  
The Application Developers Alliance  
Automattic  
Blockstream  
Cisco Systems  
Coinbase  
Cloud Linux Inc.  
CloudFlare  
Computer & Communications Industry Association  
Consumer Electronics Association (CEA)  
Context Relevant  
The Copia Institute

CREDO Mobile  
Data Foundry  
Dropbox  
Evernote  
Facebook  
Gandi.net  
Golden Frog  
Google  
HackerOne  
Hackers/Founders  
Hewlett-Packard Company  
Internet Archive  
Internet Association  
Internet Infrastructure Coalition (i2Coalition)  
Level 3 Communications  
LinkedIn  
Microsoft  
Misk.com  
Mozilla  
Open Spectrum Inc.  
Rackspace  
Rapid7  
Reform Government Surveillance  
Sonic  
ServInt  
Silent Circle  
Slack Technologies, Inc.  
Symantec  
Tech Assets Inc.  
TechNet  
Tumblr  
Twitter  
Wikimedia Foundation  
Yahoo

**Security and Policy Experts\***

Hal Abelson, Professor of Computer Science and Engineering, Massachusetts Institute of Technology  
Ben Adida, VP Engineering, Clever Inc.  
Jacob Appelbaum, The Tor Project  
Adam Back, PhD, Inventor, HashCash, Co-Founder & President, Blockstream  
Alvaro Bedoya, Executive Director, Center on Privacy & Technology at Georgetown Law  
Brian Behlendorf, Open Source software pioneer  
Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University

Matt Bishop, Professor of Computer Science, University of California at Davis  
 Matthew Blaze, Director, Distributed Systems Laboratory, University of Pennsylvania  
 Dan Boneh, Professor of Computer Science and Electrical Engineering at Stanford University  
 Eric Burger, Research Professor of Computer Science and Director, Security and Software Engineering Research Center (Georgetown), Georgetown University  
 Jon Callas, CTO, Silent Circle  
 L. Jean Camp, Professor of Informatics, Indiana University  
 Richard A. Clarke, Chairman, Good Harbor Security Risk Management  
 Gabriella Coleman, Wolfe Chair in Scientific and Technological Literacy, McGill University  
 Whitfield Diffie, Dr. sc. techn., Center for International Security and Cooperation, Stanford University  
 David Evans, Professor of Computer Science, University of Virginia  
 David J. Farber, Alfred Filter Moore Professor Emeritus of Telecommunications, University of Pennsylvania  
 Dan Farmer, Security Consultant and Researcher, Vicious Fishes Consulting  
 Rik Farrow, Internet Security  
 Joan Feigenbaum, Department Chair and Grace Murray Hopper Professor of Computer Science Yale University  
 Richard Forno, Jr. Affiliate Scholar, Stanford Law School Center for Internet and Society  
 Alex Fowler, Co-Founder & SVP, Blockstream  
 Jim Fruchterman, Founder and CEO, Benetech  
 Daniel Kahn Gillmor, ACLU Staff Technologist  
 Robert Graham, creator of BlackICE, sidejacking, and masscan  
 Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society  
 Matthew D. Green, Assistant Research Professor, Johns Hopkins University Information Security Institute  
 Robert Hansen, Vice President of Labs at WhiteHat Security  
 Lance Hoffman, Director, George Washington University, Cyber Security Policy and Research Institute  
 Marcia Hofmann, Law Office of Marcia Hofmann  
 Nadim Kobeissi, PhD Researcher, INRIA  
 Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology  
 Nadia Heninger, Assistant Professor, Department of Computer and Information Science, University of Pennsylvania  
 David S. Isenberg, Producer, Freedom 2 Connect  
 Douglas W. Jones, Department of Computer Science, University of Iowa  
 Susan Landau, Worcester Polytechnic Institute  
 Gordon Fyodor Lyon, Founder, Nmap Security Scanner Project  
 Aaron Massey, Postdoctoral Fellow, School of Interactive Computing, Georgia Institute of Technology  
 Jonathan Mayer, Graduate Fellow, Stanford University  
 Jeff Moss, Founder, DEF CON and Black Hat security conferences

Peter G. Neumann, Senior Principal Scientist, SRI International Computer Science Lab,  
Moderator of the ACM Risks Forum  
Ken Pfeil, former CISO at Pioneer Investments  
Ronald L. Rivest, Vannevar Bush Professor, Massachusetts Institute of Technology  
Paul Rosenzweig, Professorial Lecturer in Law, George Washington University School of  
Law  
Jeffrey I. Schiller, Area Director for Security, Internet Engineering Task Force (1994-  
2003), Massachusetts Institute of Technology  
Bruce Schneier, Fellow, Berkman Center for Internet and Society, Harvard Law School  
Micah Sherr, Assistant Professor of Computer Science, Georgetown University  
Adam Shostack, author, “Threat Modeling: Designing for Security”  
Eugene H. Spafford, CERIAS Executive Director, Purdue University  
Alex Stamos, CISO, Yahoo  
Geoffrey R. Stone, Edward H. Levi Distinguished Service Professor of Law, The  
University of Chicago  
Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia  
Institute of Technology  
C. Thomas (Space Rogue), Security Strategist, Tenable Network Security  
Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker  
Institute of Public Policy  
Nicholas Weaver, Researcher, International Computer Science Institute  
Chris Wysopal, Co-Founder and CTO, Veracode, Inc.  
Philip Zimmermann, Chief Scientist and Co-Founder, Silent Circle

\*Affiliations provided only for identification purposes.