January 11, 2015

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

Access Now
1110 Vermont Avenue NW
Suite 500
Washington, DC 20005

Dear President Obama,

We urge you to protect the security of your citizens, your economy, and your government by supporting the development and use of secure communications tools and technologies, rejecting policies that would prevent or undermine the use of strong encryption, and urging other leaders to do the same.

Encryption tools, technologies, and services are essential to protect against harm and to shield our digital infrastructure and personal communications from unauthorized access. The ability to freely develop and use encryption provides the cornerstone for today's global economy. Economic growth in the digital age is powered by the ability to trust and authenticate our interactions and communicate and conduct business securely, both within and across borders.

Some of the most noted technologists and experts on encryption recently explained that laws or policies that undermine encryption would "force a U-turn from the best practices now being deployed to make the Internet more secure," "would substantially increase system complexity" and raise associated costs, and "would create concentrated targets that could attract bad actors."[1] The absence of encryption facilitates easy access to sensitive personal data, including financial and identity information, by criminals and other malicious actors. Once obtained, sensitive data can be sold, publicly posted, or used to blackmail or embarrass an individual. Additionally, insufficiently encrypted devices or hardware are prime targets for criminals.

The United Nations Special Rapporteur for freedom of expression has noted, "encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."[2] As we move toward connecting the next billion users, restrictions on encryption in any country will

[1] Harold Abelson et al., *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology Technical Report (July 6, 2015).
[2] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, U.N. Doc.A/HRC/29/32 (May 22, 2015) (by David Kaye).

likely have global impact. Encryption and other anonymizing tools and technologies enable lawyers, journalists, whistleblowers, and organizers to communicate freely across borders and to work to better their communities. It also assures users of the integrity of their data and authenticates individuals to companies, governments, and one another.
We encourage you to support the safety and security of users by strengthening the integrity of communications and systems. All governments should reject laws, policies, or other mandates or practices, including secret agreements with companies, that limit access to or undermine encryption and other secure communications tools and technologies. Users should have the option to use – and companies the option to provide – the strongest encryption available, including end-to-end encryption, without fear that governments will compel access to the content, metadata, or encryption keys without due process and respect for human rights. Accordingly:

- Governments should not ban or otherwise limit user access to encryption in any form or otherwise prohibit the implementation or use of encryption by grade or type;
- Governments should not mandate the design or implementation of "backdoors" or vulnerabilities into tools, technologies, or services;
- Governments should not require that tools, technologies, or services are designed or developed to allow for third-party access to unencrypted data or encryption keys;
- Governments should not seek to weaken or undermine encryption standards or intentionally influence the establishment of encryption standards except to promote a higher level of information security. No government should mandate insecure encryption algorithms, standards, tools, or technologies; and
- Governments should not, either by private or public agreement, compel or pressure an entity to engage in activity that is inconsistent with the above tenets.

Strong encryption and the secure tools and systems that rely on it are critical to improving cybersecurity, fostering the digital economy, and protecting users. Our continued ability to leverage the internet for global growth and prosperity and as a tool for organizers and activists requires the ability and the right to communicate privately and securely through trustworthy networks.

We look forward to working together toward a more secure future.

Sincerely,

Organizations

Access Now
ACI-Participa
Advocacy for Principled Action in Government
Alternative Informatics Association
Alternatives
American Civil Liberties Union
The Global Network Initiative (GNI)
Global Voices Advox
Government Accountability Project
Hiperderecho
Hivos
Human Rights Foundation

American Library Association
Amnesty International
ARTICLE 19
Asociación por los Derechos Civiles
Asociatia pentru Tehnologie si Internet (ApTI)
Association for Progressive Communications (APC)
Australian Lawyers for Human Rights
Australian Privacy Foundation
Benetech
Bill of Rights Defense Committee
Bits of Freedom
Blueprint for Free Speech
Bolo Bhi
the Centre for Communication Governance at National Law University Delhi
Center for Democracy and Technology
Center for Digital Democracy
Center for Financial Privacy and Human Rights
the Center for Internet and Society (CIS)
Center for Media, Data and Society at the School of Public Policy of Central European University
Center for Technology and Society at FGV Rio Law School
Chaos Computer Club
CivSource
Committee to Protect Journalists
Constitutional Alliance
Constitutional Communications
Consumer Action
Consumer Federation of America
Consumer Watchdog
ContingenteMX
Críptica
Defending Dissent Foundation
Digitalcourage
Digitale Gesellschaft
Digital Empowerment Foundation
Digital Rights Foundation
DSS216
Electronic Frontier Finland
Electronic Frontier Foundation
Electronic Frontiers Australia
Electronic Privacy Information Center
Engine
Enjambre Digital
Eticas Research and Consulting
Human Rights Watch
Institute for Technology and Society of Rio (ITS Rio)
Instituto Demos
the International Modern Media Institute (IMMI)
Internet Democracy Project
IPDANDETEC
IT-Political Association of Denmark
Jonction
Karisma Foundation
Keyboard Frontline
Korean Progressive Network Jinbonet
Localization Lab
Media Alliance
Modern Poland Foundation
Myanmar ICT for Development Organization (MIDO)
Net Users' Rights Protection Association (NURPA)
New America's Open Technology Institute
Niskanen Center
One World Platform Foundation
OpenMedia
Open Net Korea
Open Rights Group
Panoptykon Foundation
Paradigm Initiative Nigeria
Patient Privacy Rights
PEN American Center
PEN International
Point of View
Privacy International
Privacy Rights Clearinghouse
Privacy Times
Protection International
La Quadrature du Net
R3D (Red en Defensa de los Derechos Digitales)
R Street Institute
Reinst8
Restore the Fourth
RootsAction.org
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
Security First
SFLC.in
Share Foundation
Simply Secure
Social Media Exchange (SMEX)
SonTusDatos (Artículo 12, A.C.)

European Digital Rights
Fight for the Future
Föreningen för digitala fri- och rättigheter (DFRI)
Freedom House
Freedom of the Press Foundation
Freedom to Read Foundation
Free Press
Free Press Unlimited
Free Software Foundation
Fundacion Acceso
Future of Privacy Forum
Future Wise
Globe International Center
Student Net Alliance
Sursiendo
Comunicación y Cultura Digital
TechFreedom
Tully Center for Free Speech at Syracuse University
Usuarios Digitales
Viet Tan
Vrijschrift
WITNESS
World Privacy Forum
X-Lab
Xnet
Zimbabwe Human Rights Forum

Companies

CloudFlare
Computer & Communications Industry Association
DuckDuckGo
HackerOne
HasGeek
Internet Association
Internet Infrastructure Coalition (i2coalition)
MediaNama
Neurocrypto, LLC
Silent Circle
Sonic

Individuals

Jacob Appelbaum
Collin Anderson
Matt Blaze
Paul Bernal
Owen Blacker
Eva Bognar
Sara Sinclair Brody
Eric Burger
Jon Callas
L. Jean Camp
Ronald Deibert
Lina Dencik
Thomas Drake
Dr. Suelette Dreyfus
David Evans
Jim Fruchterman
Mike Godwin
Matthew Green
Joseph Lorenzo Hall
Arne Hintz
Deborah Hurley
Birgitta Jonsdottir
David Kaye
Frank La Rue
Timothy Libert
Rebecca MacKinnon
Morgan Marquis-Boire
Maxigas
Bailey McCann
Andrew McLaughlin
Sascha Meinrath
Eric Mill
Katie Moussouris
Jacobo Nájera
Nikhil Pahwa
Chip Pitts
Jesús Robles Maloof
Phillip Rogaway
Marc Rotenberg
Bruce Schneier
'Gbenga Sesan
Micah Sherr
Adam Shostack
Barbara Simons
Norman Solomon
Tim Sparapani

Ephraim Percy Kenyanito
Eric King
John Kiriakou
Douwe Korff
Ryan Lackey
Susan Landau
Ritu Srivastava
Maria Swietlik
Nabiha Syed
Trevor Timm
Meredith Whittaker