

January 11, 2016

To the leaders of the world's governments –

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.

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).

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 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

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).

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	The Global Network Initiative (GNI)
ACI-Participa	Global Voices Advox
Advocacy for Principled Action in Government	Government Accountability Project
Alternative Informatics Association	Hiperderecho
Alternatives	Hivos
American Civil Liberties Union	Human Rights Foundation
American Library Association	Human Rights Watch
Amnesty International	Institute for Technology and Society of Rio (ITS Rio)
ARTICLE 19	Instituto Demos
Asociación por los Derechos Civiles	the International Modern Media Institute (IMMI)
Asociatia pentru Tehnologie si Internet (ApTI)	Internet Democracy Project
Association for Progressive Communications (APC)	IPDANDETEC
Australian Lawyers for Human Rights	IT-Political Association of Denmark

Australian Privacy Foundation	Jonction
Benetech	Karisma Foundation
Bill of Rights Defense Committee	Keyboard Frontline
Bits of Freedom	Korean Progressive Network Jinbonet
Blueprint for Free Speech	Localization Lab
Bolo Bhi	Media Alliance
the Centre for Communication Governance	Modern Poland Foundation
at National Law University Delhi	Myanmar ICT for Development Organization
Center for Democracy and Technology	(MIDO)
Center for Digital Democracy	Net Users' Rights Protection Association
Center for Financial Privacy and Human	(NURPA)
Rights	New America's Open Technology Institute
the Center for Internet and Society (CIS)	Niskanen Center
Center for Media, Data and Society at the	One World Platform Foundation
School of Public Policy of Central European	OpenMedia
University	Open Net Korea
Center for Technology and Society at FGV	Open Rights Group
Rio Law School	Panoptykon Foundation
Chaos Computer Club	Paradigm Initiative Nigeria
CivSource	Patient Privacy Rights
Committee to Protect Journalists	PEN American Center
Constitutional Alliance	PEN International
Constitutional Communications	Point of View
Consumer Action	Privacy International
Consumer Federation of America	Privacy Rights Clearinghouse
Consumer Watchdog	Privacy Times
ContingenteMX	Protection International
Crítica	La Quadrature du Net
Defending Dissent Foundation	R3D (Red en Defensa de los Derechos
Digitalcourage	Digitales)
Digitale Gesellschaft	R Street Institute
Digital Empowerment Foundation	Reinst8
Digital Rights Foundation	Restore the Fourth
DSS216	RootsAction.org

Electronic Frontier Finland
Electronic Frontier Foundation
Electronic Frontiers Australia
Electronic Privacy Information Center
Engine
Enjambre Digital
Eticas Research and Consulting
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

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.)
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
Ephraim Percy Kenyanito
Eric King
John Kiriakou
Douwe Korff
Ryan Lackey
Susan Landau

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
Ritu Srivastava
Maria Swietlik
Nabiha Syed
Trevor Timm
Meredith Whittaker

For the most up to date list of signers, please visit, <https://www.securetheinternet.org>.