June 30, 2017

Senator the Hon. George Brandis
Attorney General of Australia

Hon. Christopher Finlayson
Attorney General of New Zealand

Hon. Ralph Goodale
Minister of Public Safety and Emergency Preparedness of Canada

Hon. John Kelly
United States Secretary of Homeland Security

Rt. Hon. Amber Rudd
Secretary of State for the Home Department, United Kingdom

CC: **Hon. Peter Dutton**, Minister for Immigration and Border Protection, Australia;
Hon. Ahmed Hussen, Minister of Immigration, Refugees, and Citizenship, Canada;
Hon. Jeff Sessions, Attorney General for the United States;
Hon. Jody Wilson-Raybould, Minister of Justice and Attorney General, Canada;
Hon. Michael Woodhouse, Minister of Immigration, New Zealand

To Ministers Responsible for the Five Eyes Security Community,

In light of public reports about this week's meeting between officials from your agencies, the undersigned individuals and organizations write to emphasize the importance of national policies that encourage and facilitate the development and use of strong encryption. We call on you to respect the right to use and develop strong encryption and commit to pursuing any additional dialogue in a transparent forum with meaningful public participation.

This week's Five Eyes meeting (comprised of Ministers from the United States, United Kingdom, New Zealand, Canada, and Australia) discussed "plans to press technology firms to share encrypted data with security agencies" and hopes to achieve "a common position on the extent of … legally imposed obligations on … device-makers and social media companies to co-operate."[1] In a Joint Communiqué following the meeting, participants committed to exploring shared solutions to the perceived impediment posed by encryption to investigative objectives.[2]

While the challenges of modern day security are real, such proposals threaten the integrity and security of general purpose communications tools relied upon by international commerce, the free press, governments, human rights advocates, and individuals around the world.

Last year, many of us joined several hundred leading civil society organizations, companies, and prominent individuals calling on world leaders to protect the development of strong cryptography. This protection demands an unequivocal rejection of 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.[3]

Today, we reiterate that call with renewed urgency. We ask you to protect the security of your citizens, your economies, and your governments by supporting the development and use of secure communications tools and technologies, by rejecting policies that would prevent or undermine the use of strong encryption, and by urging other world leaders to do the same.

1. https://www.nytimes.com/reuters/2017/06/25/technology/25reuters-australia-security-messaging.html and http://www.theage.com.au/federal-politics/political-news/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html.

2. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/fv-cntry-mnstrl-2017-en.pdf.

3. We have included a copy of that statement and its signatories to this letter, which can also be found at https://securetheinternet.org.

Attempts to engineer "backdoors" or other deliberate weaknesses into commercially available encryption software, to require that companies preserve the ability to decrypt user data, or to force service providers to design communications tools in ways that allow government interception are both shortsighted and counterproductive. The reality is that there will always be some data sets that are relatively secure from state access. On the other hand, leaders must not lose sight of the fact that even if measures to restrict access to strong encryption are adopted within Five Eyes countries, criminals, terrorists, and malicious government adversaries will simply switch to tools crafted in foreign jurisdictions or accessed through black markets.[4] Meanwhile, innocent individuals will be exposed to needless risk.[5] Law-abiding companies and government agencies will also suffer serious consequences.[6] Ultimately, while legally discouraging encryption might make some useful data available in some instances, it has by no means been established that such steps are necessary or appropriate to achieve modern intelligence objectives.

Notably, government entities around the world, including Europol and representatives in the U.S. Congress, have started to recognize the benefits of encryption and the futility of mandates that would undermine it.[7]

We urge you, as leaders in the global community, to remember that encryption is a critical tool of general use. It is neither the cause nor the enabler of crime or terrorism. As a technology, encryption does far more good than harm. We therefore ask you to prioritize the safety and security of individuals by working to strengthen the integrity of communications and systems. As an initial step we ask that you continue any engagement on this topic in a multi-stakeholder forum that promotes public participation and affirms the protection of human rights.

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

Sincerely,
83 civil society organizations and eminent individuals *(listed below)*

4. https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf. Such efforts will affect law-abiding individuals more aggressively than malicious actors as the latter are more likely to seek out and find secure cryptographic alternatives.

5. Discouraging the use of encryption facilitates unauthorized 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, exploit, or humiliate an individual. Finally, at a time of ever-growing cybersecurity threats, strong encryption tools are also necessary for the work of human rights activists across the globe. *See*, https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/; *See also* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

6. Imposing limits on the availability of strong encryption technology or requiring device manufacturers and technology firms to assist governments in gaining access to encrypted data threatens the security of international commerce and business. Economic growth in the digital age is powered by the ability to conduct business securely—both within and across borders. The largest companies in the world rely on strong encryption to ensure trust, authenticate digital interactions, protect financial transactions and their own intellectual property, and maintain the confidentiality of user data. Compelling technology companies to undermine the security of their users will inevitably undermine customer trust in those services. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html. States are equally reliant on strong encryption and technical security: encryption protects the integrity of critical national infrastructure, shields sensitive government data, and preserves the confidentiality of law enforcement and intelligence investigations.

7. A statement on encryption-based challenges to investigative capabilities issued jointly by ENISA and Europol in 2016 concluded that "intentionally weaken[ing] technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well." https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0. An Encryption Working Group of the United States House Judiciary & House Energy and Commerce Committees observed that "any measure that weakens encryption works against the national interest." https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf. The former U.S. President's Review Group on Intelligence and Communications Technology concluded in late 2013 that the Government should actively encourage, rather than discourage, widespread adoption of strong cryptography, a conclusion endorsed by many of the world's largest technology companies. https://cdn.arstechnica.net/wp-content/uploads/2015/05/cryptoletter.pdf. In a draft 2017 report, the European Parliament's LIBE committee has proposed requiring—rather than undermining—end-to-end encryption in electronic communication services: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN, proposed amendment 116. It should be noted that leading technical security experts have similarly concluded that exceptional state access to encrypted data cannot be achieved without a correlating exposure to malicious actors: https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

Organizations

Access Now
Advocacy for Principled Action in Government
Amnesty International
Amnesty UK
ARTICLE 19
Australian Privacy Foundation
Big Brother Watch
Blueprint for Free Speech
British Columbia Civil Liberties Association (BCCLA)
Canadian Civil Liberties Association (CCLA)
Canadian Journalists for Free Expression (CJFE)
Center for Democracy and Techology
Centre for Free Expression, Ryerson University
Chaos Computer Club (CCC)
Constitutional Alliance
Consumer Action
CryptoAustralia
Crypto.Quebec
Defending Rights and Dissent
Demand Progress
Digital Rights Watch
Electronic Frontier Foundation
Electronic Frontiers Australia
Electronic Privacy Information Center
Engine
Equalit.ie
Freedom of the Press Foundation
Friends of Privacy USA
Future Wise
Government Accountability Project
Human Rights Watch
i2Coalition
Index on Censorship
International Civil Liberties Monitoring Group (ICLMG)
Internet NZ
Liberty
Liberty Coalition
Liberty Victoria
Library Freedom Project
My Private Network
New America's Open Technology Institute
NZ Council for Civil Liberties
OpenMedia
Open Rights Group (ORG)
NEXTLEAP
Niskanen Center
Patient Privacy Rights
PEN International
Privacy International
Privacy Times
Private Internet Access
Restore the Fourth
Reporters Without Borders
Rights Watch (UK)
Riseup Networks
R Street Institute
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
Scottish PEN
Subgraph
Sunlight Foundation
TechFreedom
Tech Liberty
The Tor Project
Voices-Voix
World Privacy Forum

Individuals

Brian Behlendorf | Executive Director, Hyperledger, at the Linux Foundation

Dr. Paul Bernal | Lecturer in IT, IP and Media Law, UEA Law School

Owen Blacker | Founder and director, Open Rights Group; founder, NO2ID

Thorsten Busch | Lecturer & Senior Research Fellow, University of St. Gallen

Gabriella Coleman | Wolfe Chair in Scientific and Technological Literacy at McGill University

Sasha Costanza-Chock | Associate Professor of Civic Media, MIT

Dave Cox | CEO, Liquid VPN

Ron Deibert | The Citizen Lab, Munk School of Global Affairs

Nathan Freitas | Guardian Project

Dan Gillmor | Professor of Practice, Walter Cronkite School of Journalism and Mass Communication, Arizona State University

Adam Molnar | Lecturer In Criminology, Deakin University

Christopher Parsons | The Citizen Lab, Munk School of Global Affairs

Jon Penney | Research Fellow, The Citizen lab, Munk School of Global Affairs

Chip Pitts | Professorial Lecturer, Oxford University

Ben Robinson | Directory, Outside the Box Technology Ltd and Discovery Technology Ltd

Sarah Myers West | Doctoral Candidate at the Annenberg School for Communication and Journalism

J.M. Porup | Journalist

Lokman Tsui | Assistant Professor at the School of Journalism and Communication, the Chinese University of Hong Kong (Faculty Associate, Berkman Klein Center)

Attachment

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 (PDF) 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." 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." 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 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.
Securetheinternet.org Signatories