

P.O. Box 4278
Sydney NSW 2001
Australia
Tel: +61-26-9114-1764

August 3, 2017

Hon. Malcolm Turnbull MP
Prime Minister
Parliament House
CANBERRA ACT 2600

Re: Encryption and Human Rights

Dear Prime Minister Turnbull,

We write to urge you to support the use of strong encryption as essential to security and human rights in the digital age. We call on you to refrain from forcing technology companies to weaken the security of their products or banning the use of end-to-end encryption.

In a July 14 press conference on national security and encryption, you discussed challenges that Australian law enforcement and intelligence agencies faced in accessing encrypted data or communications, even with a lawful court order. You announced your intention to introduce legislation that “will in particular impose an obligation upon device manufacturers and upon service providers to provide appropriate assistance to intelligence and law enforcement on a warranted basis,” to access data in unencrypted form. While the conference released few details, you stated that the legislation would be modelled on the United Kingdom’s Investigatory Powers Act and that you will seek a coordinated approach with international partners, including the Five Eyes intelligence alliance.

Governments have a human rights obligation to investigate and prosecute crime and thwart terrorist attacks. However, any policy response should not do more harm than good, while also be effective at achieving its aim. Forcing companies to weaken encryption or effectively forbidding the use of end-to-end encryption fails on both counts, and would undermine human rights worldwide.

Strong encryption is the cornerstone of cybersecurity in the digital age. Today’s cybercriminals are increasingly sophisticated, targeting Internet companies, credit card and identity data, critical infrastructure, and even

HUMAN
RIGHTS
WATCH

HRW.org

Kenneth Roth, Executive Director

DEPUTY EXECUTIVE DIRECTORS

Michele Alexander, *Development and Global Initiatives*
Nicholas Dawes, *Media*
Iain Levine, *Program*
Chuck Lustig, *Operations*
Bruno Stagno Ugarte, *Advocacy*

Emma Daly, *Communications Director*
Dinah PoKempner, *General Counsel*
James Ross, *Legal and Policy Director*

DIVISION AND PROGRAM DIRECTORS

Brad Adams, *Asia*
Maria McFarland Sánchez-Moreno, *United States*
Alison Parker, *United States*
Mausi Segun, *Africa*
José Miguel Vivanco, *Americas*
Sarah Leah Whitson, *Middle East and North Africa*
Hugh Williamson, *Europe and Central Asia*

Shantha Rau Barriga, *Disability Rights*
Peter Bouckaert, *Emergencies*
Zama Neff, *Children’s Rights*
Richard Dicker, *International Justice*
Bill Frelick, *Refugees’ Rights*
Arvind Ganesan, *Business and Human Rights*
Liesl Gernholtz, *Women’s Rights*
Steve Goose, *Arms*
Diederik Lohman, *Health and Human Rights*
Marcos Orellana, *Environment and Human Rights*
Graeme Reid, *Lesbian, Gay, Bisexual, and Transgender Rights*

ADVOCACY DIRECTORS

Maria Laura Canineu, *Brazil*
Louis Charbonneau, *United Nations, New York*
Kanae Doi, *Japan*
John Fisher, *United Nations, Geneva*
Meenakshi Ganguly, *South Asia*
Bénédicte Jeannerod, *France*
Lotte Leicht, *European Union*
Sarah Margon, *Washington, DC*
David Mepham, *United Kingdom*
Wenzel Michalski, *Germany*
Elaine Pearson, *Australia*

BOARD OF DIRECTORS

Hassan Elmasry, *Co-Chair*
Robert Kissane, *Co-Chair*
Michael Fisch, *Vice-Chair*
Oki Matsumoto, *Vice-Chair*
Amy Rao, *Vice-Chair*
Amy Towers, *Vice-Chair*
Catherine Zennström, *Vice-Chair*
Michael Fisch, *Treasurer*
Bruce Rabb, *Secretary*
Karen Herskovitz Ackman
Akwas Aidoo
Jorge Castañeda
Michael E. Gellert
Leslie Gilbert-Lurie
Paul Gray
Betsy Karel
David Lakhdir
Kimberly Marteau Emerson
Alicia Miñana
Joan R. Platt
Neil Rimer
Shelley Frost Rubin
Ambassador Robin Sanders
Jean-Louis Servan-Schreiber
Sidney Sheinberg
Bruce Simpson
Joseph Skrzynski
Donna Slaight
Siri Stolt-Nielsen
Darian W. Swig
Makoto Takano
Marie Warburg

nation-state intelligence agencies.¹ Strong encryption built into private sector technology protects the data—and the human rights and security—of billions of Internet users worldwide against these growing security threats. You yourself have acknowledged that you use encrypted applications like Wickr and WhatsApp because traditional communication methods are not secure.²

Weakening encryption for any purpose effectively weakens it for every purpose, including malicious hacking, financial fraud, and for other illicit purposes. And unfortunately, weak or partial encryption provides not just weak or partial protection, but no protection at all against sophisticated repressive regimes and capable criminals. Some companies that manufacture encrypted apps or devices do not have the ability to disclose conversations or data to law enforcement because that information is encrypted “end-to-end” and companies do not have the decryption keys. A requirement of assured decryptability for all data would force such companies to redesign their products without security features like end-to-end encryption or to introduce deliberate vulnerabilities, or “back doors,” into their software.

The overwhelming consensus of information security experts, along with some former Five Eyes intelligence officials, is that there is no technical solution that would allow specific law enforcement agencies to decrypt communications without creating vulnerabilities that would expose all users to harm.³ Europol has also warned that “solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically

¹ See, for example, Sam Thielman, "Yahoo hack: 1bn accounts compromised by biggest data breach in history," *The Guardian*, December 15, 2016, <https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached> (accessed August 2, 2017); Nicole Perlroth & David Sanger, "Hacks Raise Fear Over N.S.A.'s Hold on Cyberweapons," *New York Times*, June 28, 2017, <https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html> (accessed August 2, 2017).

² Eliza Borrello, "Malcolm Turnbull confirms he uses Wickr, WhatsApp instead of unsecure SMS technology," ABC News, March 2, 2015, <http://www.abc.net.au/news/2015-03-03/malcolm-turnbull-uses-secret-messaging-app-instead-of-sms/6276712> (accessed August 2, 2017).

³ Nicole Perlroth, "Security Experts Oppose Government Access to Encrypted Communication," *New York Times*, July 7, 2015, <https://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html> (accessed August 2, 2017); Mike McConnell, Michael Chertoff and William Lynn, "Why the fear over ubiquitous data encryption is overblown," July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html (accessed August 2, 2017); John Leyden, "Former GCHQ boss backs end-to-end encryption," *The Register*, July 10, 2017, https://www.theregister.co.uk/2017/07/10/former_gchq_wades_into_encryption_debate (accessed August 2, 2017).

weaken the protection against criminals as well.”⁴ Determined cybercriminals and rival foreign intelligence agencies will find and exploit such back doors, for profit or abuse. This would undermine cybersecurity for all users, including billions that are under no suspicion of wrongdoing.

For human rights defenders and journalists, the harm can be even more serious. Activists and media organizations with whom we work in places like Hong Kong, Vietnam, Thailand, and across the Middle East rely on encryption built into phones and chat applications to protect sources and victims from reprisals. In 2015, the UN special rapporteur on freedom of expression, David Kaye, recognized that encryption enables the exercise of freedom of expression, privacy, and a range of other rights in the digital age.⁵ Countries like Russia, China, and Turkey need no encouragement, they are already blurring the line between human rights activism and terrorism in order to justify surveillance and repression of human rights activists.

While strong encryption may limit some existing surveillance capabilities, weakening such security features will only increase the vulnerability of billions of ordinary people to cybercrime, identity theft, and malicious hacking. Such harm would be broadly disproportionate to any gains in law enforcement capabilities that undermining encryption would achieve.

It is also unlikely that limiting strong encryption in Australia—or even in all Five Eyes countries— would prevent bad actors from using it. As a recent global survey of encryption products confirms, terrorists and criminals could easily shift to the many available foreign alternatives that would not be subject to Australian law.⁶

Technology companies face an escalating digital arms race to secure their software and devices against cybercriminals, and encryption is a key part of their arsenal. Instead of hindering efforts to protect ordinary users, we urge your government to invest in modernizing investigation techniques and increasing resources and training in tools

⁴ Europol and ENISA joint statement, "On lawful criminal investigation that respects 21st Century data protection," May 20, 2016, <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection> (accessed August 2, 2017).

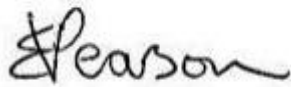
⁵ UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, May 22, 2015, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 (accessed August 2, 2017).

⁶ B. Schneier, K. Seidel, and S. Vijayakumar, A Worldwide Survey of Encryption Products, February 11, 2016, https://www.schneier.com/academic/archives/2016/02/a_worldwide_survey_o.html (accessed August 2, 2017).

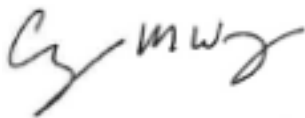
already at their disposal, consistent with human rights requirements.⁷ For example, any limitations encryption poses to police capabilities are greatly offset by the explosion of new kinds of investigatory material enabled by the digital world, including location information and vast stores of metadata that are not encrypted. And encrypted data can often be accessed in unencrypted form through cloud-based backups or by directly accessing it on devices with hacking or forensic tools. Of course, these alternative approaches should also be necessary and proportionate to legitimate security goals, regulated in public law, and subject to strict safeguards to ensure respect for privacy and other rights.

Australia's approach to encryption will be emulated by other countries facing similar challenges. Your government can demonstrate true leadership by adapting to a world with strong encryption instead of fighting the gains the private sector has made in shoring up security and human rights in the digital age.

Sincerely,



Elaine Pearson
Australia Director



Cynthia Wong
Senior Internet Researcher

CC:

Senator the Hon. George Brandis QC, Attorney-General

Mr. Michael Phelan APM, Acting Commissioner of the Australian Federal Police

⁷ Orin Kerr and Bruce Schneier, Encryption Workarounds, March 20, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033 (accessed August 2, 2017).