17 July 2018

Senator the Honorable Scott Ryan
President of the Senate
Parliament of Australia
PO Box 6100
Senate
Parliament House
Canberra ACT 2600

Honorable Tony Smith MP
Speaker of the House of Representatives
Parliament of Australia
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

cc: Honorable Christian Porter MP
Attorney-General for Australia
Commonwealth Parliamentary Offices
Exchange Plaza
2 The Esplanade
Perth WA 6000

cc: Honorable Mark Dreyfus QC, MP
Shadow Attorney-General for Australia
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

cc: Honorable Angus Taylor MP
Minister for Law Enforcement and Cyber Security
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

To Whom It May Concern:

The undersigned domestic and international organizations and experts write today to urge you to protect Australia's cybersecurity. Specifically, we ask you not to pursue legislation that would undermine tools, policies, and technologies critical to protecting individual rights, safeguarding the economy, and providing security both in Australia and around the world.[1] Further, we encourage you to publicly affirm your support for strong encryption.

In early June, Minister for Law Enforcement and Cyber Security, Honorable Angus Taylor MP, gave a speech asserting, "there will [...] need to be obligations on industry – telecommunications and technology service providers – to cooperate with agencies to get access to [encrypted] data."[2] Notably, he clarified that the Australian government would not seek to require "access to a decryption key otherwise under the sole control of a user."[3]

While the apparent commitment to avoid an escrow system for encryption keys is a positive step, we note that, generally speaking, all known methods of bypassing, altering, or watering down security tools or technologies to provide law enforcement access have been shown to carry severe risk.

For example, one idea that has been discussed is a legal compulsion for communications hardware or software providers to alter their products in some way to ensure government access.[4] This approach may include a specific alteration delineated by government officials, or a general requirement for providers to guarantee access without detailing the precise means through which this would be accomplished.[5] Another potential approach that has been discussed is a mandatory decryption requirement for companies, which would effectively prohibit companies from offering some of the strongest security tools available today, or in the future.

Adopting either of these requirements would be a mistake. While we respect the challenges facing law enforcement, changes elicited through either regime would have a deleterious impact on internet security, including for government and business officials as well as journalists and human rights defenders. Impacts would also be felt across important sectors, from banking to infrastructure, including Australia's continued investments in development and smart cities, with potential consequences seen in increases in online criminal activity and unauthorized access to personal and proprietary data.[6]

---

[1] *See* secureaustralia.org.au. *See also*, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.
[2] http://minister.homeaffairs.gov.au/angustaylor/Pages/speech-sydney-institute.aspx.
[3] *Id.*
[4] *See, e.g.*, http://www.abc.net.au/radionational/programs/drive/g20-summit:-pm-to-push-cyber-security-against-terrorism/8685536.
[5] *See, e.g.*, https://www.gov.uk/government/news/draft-technical-capability-regulations-notified-to-european-commission-following-targeted-consultation.
[6] *See*, https://northernaustralia.nt.gov.au; https://cities.infrastructure.gov.au/smart-cities-plan.

While these mandates would have serious direct effects on digital security, indirect consequences could be worse. Companies rely on user trust to ensure that they are able to retain customers and keep users engaged in updating and patching products. If users lose trust in the companies with which they interact online, both users and systems would face even greater cyber threats.[7] For example, one of those threats would be the increased conscription of out-of-date products into botnets, which could be used for anything from denying user access to critical services (relevant as Australia seeks to provide more government services through the internet[8]) to delivering additional malware to ever-increasing numbers of users or systems.[9]

We strongly agree with Senator The Hon Arthur Sinodinos AO, Australia's then-Minister for Industry, Innovation and Science, in his preface to Australia's Digital Economy Consultation Paper, "[t]he digital economy and the technologies that underpin it are fundamental for Australia's success."[10] However, in order to fully realize the benefits of the digital space, Australia must fully and unequivocally commit to a strong foundation for digital security.

It is essential sitting members of Parliament heed calls from a range of stakeholders that are collectively concerned about maintaining cybersecurity, public safety, and human rights for a nuanced solution that will not unnecessarily undermine strong security in digital communications. We strongly urge the government to commit to not only supporting, but investing in the development and use of encryption and other security tools and technologies that protect users and systems. We also urge you to advance other structures that will help secure Australia's digital future, such as the establishment of a vulnerabilities disclosure process and protection for security research.

We recognize this may impact the ability of law enforcement to readily obtain access to some types of evidence and cause them to face friction in seeking such access.[11] To mitigate these impacts in a manner that respects human rights and the rule of law, we would welcome the opportunity to engage in a dialogue on education and resources for law and policy makers, as well as law enforcement officials, to help determine what courses of action are available to gain access to evidence in a timely manner.

Thank you,

COMPANIES AND ORGANIZATIONS

Access Now

Advocacy for Principled Action in Government

ARTICLE 19

Assembly Four

Australian Privacy Foundation

Blueprint for Free Speech

Center for Democracy & Technology

Courage Foundation

CryptoAUSTRALIA

Digital Rights Watch

Electronic Frontier Foundation

Electronic Frontiers Australia

Enjambre Digital

Freedom of the Press Foundation

Future Wise

Hack for Privacy

International Civil Liberties Monitoring Group

Internet Australia

Internet Society

The Juice Media

Linux Australia Inc.

New America's Open Technology Institute

OpenMedia

Open Rights Group

Privacy International

Private Internet Access

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Startpage.com

ThoughtWorks

Twilio

Wickr

World Privacy Forum

X-Lab

[7] *See, e.g.*, https://www.troyhunt.com/dont-tell-people-to-turn-off-windows-update-just-dont/.
[8] https://www.smh.com.au/politics/federal/minister-s-bid-to-be-leader-in-digital-government-by-2025-20180612-p4zl01.html.
[9] For a description of a botnet, *see* https://usa.kaspersky.com/resource-center/threats/botnet-attacks.
[10] https://www.industry.gov.au/innovation/Digital-Economy/Documents/Digital-Economy-Strategy-Consultation-Paper.pdf.
[11] *See, e.g.*, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

17 July 2018

INDIVIDUALS

Affiliations for identity purposes only

Tim Baxter
Councillor, Canal Ward, Port Phillip Council

Dr. Paul Bernal
Senior Lecturer, UEA Law School

Owen Blacker
Founder, NO2ID, UK

L Jean Camp
Indiana University

Joanne Carson
Viral Hepatitis Clinical Research Program, Kirby Institute, UNSW

Tanja Chester

Aidan Clarke

Dr. Angela Daly
Assistant Professor, Chinese University of Hong Kong Faculty of Law
Adjunct Research Fellow Queensland University of Technology Faculty of Law

Jeremy Davis
TurnKey GNU/Linux

Susanna Duffy

Lex Edmonds
Director, Microtax Pty Ltd

Anna Fredericks
James Cook University

Barrie Frieden-Collins

Lex Gill
Research Fellow, Citizen Lab, Munk School of Global Affairs and Public Policy, at the University of Toronto

Olaf Goy

Ben Harris-Roxas
Associate Professor

Dr. Sven Herpig
Project Director of the Transatlantic Cyber Forum

Mary Kostakidis
Journalist and broadcaster

Ryan Kris
Director, Digital Serf, Sydney

C van Langenberg

Jon Lawrence

Antony Loewenstein
Independent journalist, author, and film-maker

Dr. Monique Mann
Vice-Chancellor's Research Fellow, Faculty of Law, Queensland University of Technology

Liz McIntyre
Author and Consumer Privacy Expert

Sascha Meinrath
Director, X-Lab
Palmer Chair in Telecommunications, Penn State University

Dr. Adam Molnar
Lecturer, Criminology Deakin University

Jacobo Nájera

George Newhouse
National Justice Project

Peter Palmer

Dr. Christopher Parsons
Research Associate, Citizen Lab, Munk School of Global Affairs and Public Policy, at the University of Toronto

Riana Pfefferkorn
Cryptography Fellow Stanford Center for Internet and Society

Christian W Probst
Professor Cyber Security, Unitec Institute of Technology

Stuart Rees
AM Professor Emeritus, University of Sydney

Hedimo Santana

Adam Shostack

Dr Abhay Kumar Singh, B. Tech (IT), MBA, PhD
Senior Lecturer in Finance, Macquarie University

Lachlan Simpson, Systems Administrator
EFA Board Member

Dr. Vanessa Teague
Melbourne School of Engineering, The University of Melbourne

Haydn Thompson
Kensington, VIC

Stefan Tober
Owner, Lighthouse Websites

Nic Van

Willem F. Westerbeek

Suzy Wood
Lawyer