Electronic Frontiers
AUSTRALIA

Mail GPO Box 1235, Canberra ACT 2601
Phone 02 6101 9968 Twitter @efa_oz
Web www.efa.org.au Email email@efa.org.au

Hon. Malcolm Turnbull, Prime Minister
Parliament House Canberra ACT 2600

cc: Hon Bill Shorten, Leader of the Opposition; Hon Senator George Brandis QC, Attorney-General; Hon. Mark Dreyfus QC, Shadow Attorney-General

18th January 2016

Re: Open letter to world leaders urging support for the safety and security of users, companies, and governments by strengthening the integrity of communications and systems.

Dear Prime Minister,

Electronic Frontiers Australia, along with the Australian Privacy Foundation, Blueprint for Free Speech and Future Wise Australia, are all signatories to an open letter to world leaders urging support for the safety and security of users, companies, and governments by strengthening the integrity of communications and systems. That letter follows below and has been, in total, signed by over 200 signatories from 43 countries and has already been delivered to Prime Minister Cameron and President Obama. Details of all signatories are available at www.securetheinternet.org.

Your own well-publicised use of encrypted communications technologies demonstrates that you clearly understand the critical importance that strong encryption plays in enabling digital activity. Encryption is of course a critical tool enabling commerce across all sectors of the economy, as well as providing the security needed for a free, unfettered media to operate and for individuals to communicate in privacy. It is also of critical importance to the operations of government.

We are alarmed by recent calls to undermine encryption technologies, including proposed legislation in certain countries, in the name of national security, and for 'backdoors' to be created to allow intelligence agencies to access nominally secure communications. Such actions threaten to undermine trust in digital communications, which will not only have serious chilling effects on free expression, but could have potentially disastrous economic impacts. Not only is strong encryption vital to protect national infrastructure (public and private), but in a democratic nation national security cannot be separated from the security of its citizens, including their right to protect their privacy, their identity, and their digital assets.

We are strong supporters of your vision for an innovative, digitally-enabled future for Australia and the world and urge you to show global leadership in resisting these misguided attempts to undermine digital security.

We do not underestimate the difficulty or complexity of the challenges that current security threats pose, however, as you meet with President Obama next week, we hope that you will bring to bear the benefit of your experience and expertise in this regard to ensure that the future of global digital activity is not compromised.

Yours Sincerely,

Jon Lawrence
Executive Officer, Electronic Frontiers Australia

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 unauthorised 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[1] 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, whistle-blowers, and organisers 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

[1] See: https://www.schneier.com/cryptography/paperfiles/paper-keys-under-doormats-CSAIL.pdf

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 organisers 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.

As of 15th January 2016, this letter had been signed by more than 200 organisations, companies and individuals from 43 countries, and is available in 13 languages.

Please refer to www.securetheinternet.org for more details and for the full list of signatories.