A Joint Call to World Leaders for a Secure and Trusted Digital Economy

World leaders, stand by these principles for a healthy digital society

World leaders, we stand by these principles for a healthy digital society and we urge you to do the same. Notably, we ask you to protect and promote strong encryption which is the foundation for our digital economies, digital societies, and interdependent lives.

Measures that undermine encryption weaken security for all.

In April 2019, G7 Ministers of the Interior expressed a commitment to encourage Internet companies to establish exceptional access[1] solutions for encrypted content. They want companies to be able to hand over the content that is communicated or stored on their services, even if it is encrypted.

This approach poses a serious threat to the ongoing security of Internet communications[2], and all those who rely on those services. It endangers citizens' trust in the security of digital products and services — calling into question their willingness to communicate, to invest, to innovate.

Our ask to you

We ask you to prioritise digital security and express your commitment not to require, coerce or persuade device manufacturers, application and service providers to:

- modify their products or services or delay patching a bug or security vulnerability to provide exceptional access to encrypted content;
- turn off "encryption-on-by-default";
- cease offering end-to-end encrypted services; or
- otherwise undermine the security of encrypted services.

Digital security is not optional. It is the foundation of our connected economies and societies. Without digital security, we can neither trust nor shape technological developments.

Strong encryption is central to digital security.

Encryption technologies keep people safe online by protecting the integrity and confidentiality of digital data and communications. They secure web browsing, online banking, and critical public

---

[1] Exceptional access, also referred to as "lawful access," refers to providing law enforcement and intelligence agencies with access encrypted communications.

[2] See: *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* – and Open Letter to GCHQ

services like electricity, elections, hospitals and transportation – and every citizen that relies on these services.

Communications on the Internet are more secure today because they are encrypted. More people are choosing end-to-end encrypted messaging apps for conversations, sharing images, conducting business and making video calls. In 2018, over 72% of all daily network traffic was encrypted and more than 1.5 billion people used E2E encrypted messaging services to protect their communications, highlighting the scale at which people now rely on secure encryption.[3]

By 2020, the Internet is estimated to contribute nearly $7 trillion USD every year to the G20 economies.[4] Exceptional access mandates put that at risk. Encryption is a vital component in protecting the new digital businesses that will shape the global economy's future, and everyone who depends on them.

National exceptional access approaches could drive customers that depend on high-assurance encryption software to look in other countries. It could also cause local markets for digital security to shrink and lead to the loss of valuable innovation in security technologies.

As you strive to tackle global inequalities at the G7 Leaders Summit and beyond, we ask you to recognize the particular importance of digital security for our digital economies and societies.

To be World Leaders in digital innovation and development, there is no room for weakening digital security.

[3] https://www.networkcomputing.com/network-security/encrypted-traffic-reaches-new-threshold and https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad/

[4] https://www.bcg.com/publications/2015/infrastructure-needs-of-the-digital-economy.aspx