INCLO CALLS ON STATES TO DEFEND END-TO-END ENCRYPTION

16 November, 2020

Fourteen members of INCLO express grave concerns regarding recent moves by various groups to break encryption. We note with alarm calls from the Council of the European Union, the European Commission, and the Department of Justice in the US, with support from Australia, Canada, New Zealand, India, Japan and the UK, to allow police authorities intercept encrypted communications.

We also draw attention to the fact that today the European Court of Human Rights communicated the case 'Telegram Messenger LLP and Telegram Messenger Inc. against Russia'[1] to the Russian Government. This is in relation to a complaint pertaining to a ban imposed by a Russian court on the online messaging service Telegram, after Telegram refused to hand over decryption keys needed to access users' confidential messages. This is the first case concerning end-to-end encryption (E2EE) to go before the ECHR who will be considering whether this ban constitutes an interference with freedom of expression and whether such an interference was necessary in a democratic society. This case will likely have a profound impact on E2EE and the balance struck between privacy and national security.

End-to-end encryption keeps us safe

E2EE is vital to protect the privacy and security of citizens and governments around the world, as E2EE prevents any third party from reading messages sent between the sender and the recipient. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression says E2EE has become the most basic building block for digital security on messaging apps with many apps offering encryption as a matter of default.

But E2EE is not just an essential tool that we use to safeguard our texts, emails, voice calls and social media. E2EE also protects and secures the processing of our data when it comes to sensitive activities

[1] Disclaimer: Agora's lawyer represents Telegram in the pending case before the European Court of Human Rights.

such as personal banking transactions, online credit card use, online shopping, buying health insurance, accessing health data, making mobile payments and carrying out our employment. Given the proliferation of "smart" technologies and our ever-growing digital footprints, E2EE provides protection from the pervasive surveillance enabled by our increasingly digitalised lives. We are alarmed that the foundation of trust that enables the digital market would be jeopardised by this measure.

Further, breaking E2EE simply will not achieve its intended purposes. It won't assist national security - experts say, "if strong encryption is outlawed, only outlaws will have strong encryption." Open source code for encrypted communication software is freely available.

For the best policy decisions to be made, better data is needed. A significant study of publicly available information has previously found that there was a lack of evidence to show that E2EE played a significant role in six major terrorist attacks (Mumbai, London, Boston, San Bernardino, Paris and Brussels, or in failed attempts in New York and Koln). Instead the attackers used surprise and responder confusion to carry out attacks. Similarly, while child abuse is horrifying, weakening E2EE for organised groups distributing child sexual abuse material is unlikely to be effective.

Meanwhile, Europol itself reported last year that official statistics on how much digital evidence is seized in criminal investigations, or on the number of investigations that require decryption of data, are not available. Without this data, how can we measure the proportionality and necessity of moves which would impact, at the very least, the more than 450 million unique mobile phone subscribers in Europe?

INCLO member alarm regarding encryption-breaking proposals

INCLO members express serious concern regarding the impact these proposals will have on the personal privacy and security of people throughout the world. The plans strike at the heart of Article 8 of the European Convention on Human Rights which protects the right to respect for private life, the home and correspondence, including the privacy of messages, phone calls and emails. Article 17 (1) of the International Covenant on Civil and Political Rights (ICCPR) also provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. No matter how carefully a technical encroachment on encryption is applied, it risks malicious attacks, serious commercial and governance consequences and weakens mechanisms used by legislators themselves.

INCLO calls on states to defend secure and private communication rights

So many of our online activities involve the transmission of highly sensitive data that is currently protected by strong encryption. Any weakening of that encryption, no matter how well intentioned, will weaken security around these activities; increase the chance of that encrypted data being accessed by malicious third parties; increase well-founded fears of fraud and identity theft; and likely breed distrust.

INCLO calls on authorities to protect E2EE and safeguard the privacy and innumerable daily security benefits and uses of encryption by people around the world.

INCLO is a network of 15 independent, national human rights organizations. Learn more at inclo.net