Brussels, 10 November 2020

Dear representatives of the German Presidency,

We are writing you to provide written feedback on behalf of European Digital Rights (EDRi) on the LIMITE document 12143/1/20.[1]

First, we support the statements in the draft document that reaffirm the need to secure encryption as the basis not only for ensuring the right to privacy but also to ensure the security of governments, companies and citizens alike. Given the importance of encryption in protecting infrastructure, we recall the need to promote the use of this technology by default:[2] software companies should be required to apply it where possible, as strongly suggested by the General Data Protection Regulation (GDPR). The use of freely available, open encryption protocols should be the universal standard. Governments must not in any way undermine the development, production or use of high-grade encryption.

Second, encryption is the basis of the security with which the majority of social, business and government transactions and relationships are conducted.[3] Thanks to encryption protocols which are widely implemented, businesses negotiate contracts, citizens submit digital tax returns and the intelligence community encrypts state secrets. Encryption takes trust from where it exists to where it is needed. Actions that undermine trust in the integrity and confidentiality of electronic information – including communications – undermine the very basis of modern digital society. As MEPs Gamon, Körner and in't Veld also refer to the Article 29 Data Protection Working Party in the letter they sent this week, "encryption is a necessity in the modern digital world. Such technologies contribute in an irreplaceable way to our privacy and to the secure and safe functioning of our societies".[4] The draft Council resolution points out that digital vulnerabilities create the potential for exploitation for criminal purposes. Indeed, any effort to mandate security flaws in technical systems will empower criminals and malicious state actors. We must maintain and strengthen the security of our societies and protect critical infrastructure and private communications alike.

Third, we fully understand the need for law enforcement agencies to legally access information in criminal investigations. This process must be based on a court order authorising access and must respect the principles of legality, transparency, necessity and proportionality, as the document suggests. Where encryption is end-to-end, and therefore traditional

1 https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf
2 See our previous submission: https://edri.org/wp-content/uploads/2020/10/20201006-EDRi-comments-to-German-Presidency-on-encryption.pdf
3 Please see EDRi's position paper on encryption: https://www.edri.org/files/20160125-edri-crypto-position-paper.pdf
4 https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51026

interception of communications is rendered useless, law-enforcement access must occur at the end points of a communication. Courts can and do grant access to information stored on both servers and end devices. Courts also can and do grant orders authorising the authorities to take down telecommunications systems that are used exclusively for criminal purposes. The suggested legal safeguards however are not enforceable if tech companies are forced to build security flaws in their systems.[5]

Fourth, we cannot accept that law enforcement and intelligence agencies should be granted the right to screen messages about to be sent from consumer devices before they are protected by end-to-end encryption. Such a program would amount to unlawful mass surveillance.[6]

Finally, we would like to highlight the need to include digital security researchers, human rights defenders and NGOs in the consultations described in paragraph 5 of the document. More and more journalists, activists (environmental groups, trade unions and human-rights defenders generally) use encryption technologies to protect themselves from authoritarian governments. These groups are key stakeholders in this debate; they should be considered as essential, and listened to as carefully, as businesses and Member State governments when debating and implementing policies related to the implementation and use of encryption technologies and the work against crime.

We therefore :

- Urge the EU and its Member States to abandon plans to weaken information security measures such as end-to-end encryption.
- Urge the EU and its Member States to refrain from mandating companies to build pre-encryption screening or other security flaws into their systems.
- Strongly advocate a targeted approach regarding access to private information. Targeted decryption or equipment-interference orders directed to specific cases should be used only when less intrusive means are not available and must only be used in exceptional circumstances to achieve a legitimate aim, based on law and clearly limited in scope.[7]
- Call for any future debates on encryption to involve human rights NGOs, digital rights experts and other civil society groups.
- Call on the European Union to invest in the development of better tools for digital forensics so that investigators can make proper use of material to which they have lawful access.

Sincerely,
Diego Naranjo
Head of Policy
European Digital Rights (EDRi)
diego.naranjo@edri.org

5 https://twitter.com/accessnow/status/1325765671742025728?s=20

6 Indeed, during the 'Crypto War' of the 1990s, it was suggested that rather than insisting on access to cryptographic keys, governments might instead insist that everyone use a cloud-based spell-checker that they controlled. That suggestion was actually a spoof, which people thought hilarious at the time. Europe should avoid falling for similar suggestions. See T Berson, "Her Majesty's Orthography Service', IHW 1996, at http://www.anagram.com/berson/abshmos.html.

7 Amnesty International USA, "Encryption as a matter of human rights", p. 40, available at https://www.amnestyusa.org/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

Signatures:
- Access Now
- Article 19
- European Digital Rights (EDRi)
- Electronic Frontier Foundation (EFF)
- epicenter.works
- FITUG e.V.
- Foundation for Information Policy Research (fipr)
- Homo Digitalis