To: Justice and Home Affairs Council
CC: Standing Committee on Operational Cooperation on Internal Security (COSI)
Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS)
Directorate General Migration and Home Affairs
European Data Protection Board
European Parliament Civil Liberties, Justice and Home Affairs Committee Chair and Group coordinators

11-12-2024

Subject: Joint letter calling for the EU digital security agenda to promote fundamental rights and support a safe digital ecosystem

Dear Ministers,

We, the undersigned professional associations, media and human rights organisations, trade unions and technology companies, are writing to you to underline the necessity of an EU digital security agenda that both ensures justice, accountability and the respect of fundamental rights, and supports the development of a safe digital ecosystem.

In this context, we would like to share our concerns as regards the recommendations and report put forward by the High-Level Group (HLG) on access to data for effective law enforcement.[1] In light of the HLG's overall aim to grant law enforcement authorities maximal access possible to personal data, we identify important risks of mass surveillance as well as substantial security and privacy threats, if these recommendations were taken as a basis for future EU policies and legislation.

We therefore urge you to consider the following recommendations when defining EU priorities in this policy area.

Respect fundamental rights and ensure the security and confidentiality of digital spaces

We would like to warn against granting law enforcement unfettered capacities that may lead to mass surveillance and violate fundamental rights.

In particular we are extremely worried about the concept of "lawful access by design"[2] supported by the HLG, which aims at mainstreaming law enforcement access to data in the development of all technologies. In practice it would require the systemic weakening of all digital security systems, including but not limited to encryption. As a result, it would undermine the security and confidentiality of electronic data and communications, put everyone's safety at risk and severely encroach people's fundamental rights. This concept goes against the long-established recommendations of human rights organisations, data protection and cybersecurity experts, as well as the European Court of Human Rights' (ECtHR) jurisprudence.[3]

We therefore recommend to discard any measure that may bypass the protections afforded by encryption or weaken them, as it would create security and privacy threats to millions of people, public institutions and inevitably damage the broader digital information ecosystem.

Furthermore, we would like to recall that any future EU harmonised regime on data retention and access[4] must respect the legal requirements of necessity and proportionality set out in EU law and the well-established case law of the Court of Justice of the EU (CJEU) and the ECtHR for the protection of fundamental rights against mass surveillance. In that regard, the proposed extension of the data retention obligation to virtually all information society services, encompassing the internet of things and internet-based services[5], is particularly concerning, as it would demand the untargeted, indiscriminate retention of personal data. This broad and general monitoring would generate in people's mind the feeling that their private life is the subject of constant surveillance and cannot be considered compliant with the aforementioned requirements.

Uphold the right to privacy and inviolability of protected information

Whilst the right to privacy and confidentiality of communications is not absolute, any interference with fundamental rights must be compliant with the principles of legality, strict necessity and proportionality. General and indiscriminate retention of personal data that allow detailed profiles of the individual to be created and measures that undermine the security of all private

1 Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en

2 Recommendations 22, 23, 25, 26

3 In PODCHASOV v. RUSSIA, the ECtHR ruled that a general obligation to weaken encryption is disproportionate in a democratic society after noting that decryption obligations "allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest."

4 Recommendations 27 to 32

5 Recommendation 27 ii

communications do not meet these principles.

Those general and indiscriminate measures also affect persons whose communication is subject to professional secrecy, such as doctors and their patients, journalists and their sources, lawyers and social workers and their clients. The legal protection granted to those communications is a sine qua non guarantee for people's effective exercise of other fundamental rights, including the right to a fair trial and of defence, freedom of expression and information including media and press freedoms, freedom of thought and religion, freedom of assembly and association, and the rights to social assistance and health care.

We are concerned that the envisaged sweeping powers for law enforcement to access data would interfere with the confidentiality of protected communications and related fundamental rights. These measures risk being abused to target journalists, human rights defenders, lawyers, activists and political dissidents. Crucially, the EU must guarantee the inviolability of data and other evidence falling under the principle of legal professional privilege or professional secrecy.

Support a safe, trustworthy and diversified digital ecosystem

Responsible device manufacturers and service providers have invested considerable resources in improving the security of their devices and the reliability of their services. These innovations not only meet the demands of increasingly privacy-conscious users, but also of regulatory authorities in charge of enforcing elevated standards in the cybersecurity and data protection fields. The EU holds a unique advantage thanks to a data protection framework that sets a high legal standard for protecting the fundamental rights and freedoms of people in a world where privacy is under constant attack.

Unfortunately, the HLG's vision could undermine Europeans' ability to choose trustworthy digital tools in the future. It recommends to set extensive, and sometimes contradictory, obligations on operators. This includes forcing them to collect and retain more user data than what is needed for providing their services, enabling real time interception[6] and providing decrypted data to law enforcement, all the while avoiding to compromise the security of their systems. Despite the HLG's intention to not undermine digital security, there is in reality no technical way to break the promise of end-to-end encryption without weakening the security of communications systems. A backdoor - or any other circumvention mechanism - intended for law enforcement can always be exploited by other actors, as numerous examples have shown.[7]

Lastly, the HLG also outlines a worrying enforcement framework, including harsh sanctions to deter and punish non-compliance with EU obligations and law enforcement orders (administrative sanctions, commercial ban, imprisonment).[8] We see here the risk of either driving reliable operators offering secure services out of the EU market or out of business if they are small or not-for-profit, or preventing them from developing secure solutions if established in the EU. Needless to say, this would be highly detrimental to the EU's cybersecurity initiatives and ambitions.

---

6 Recommendation 38

7 For example, the built-in vulnerabilities of TLS/SSL protocols affected government websites for a decade before being patched in 2015: https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/. Other examples include the hack of the lawful interception facilities of Vodafone in Greece called "The Athens Affair" which enabled the eavesdropping of over 100 politicians, with serious consequences for national security. Another recent example is the massive cyberattack that penetrated United States broadband networks, including AT&T and Verizon, through the channels used by the United States government to engage in court authorised broadband network wiretaps: https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

8 Recommendations 33 to 36

We understand that investigative measures available to law enforcement must be adequate for the digital age and effective in addressing the unique challenges created by cross-border online services. However, efficiency should not be achieved at the expense of weakening fundamental rights, legal safeguards and the European economy. We are convinced that these objectives of general interest can be met with less intrusive measures than mass surveillance and systemic weakening of essential security guarantees.

We thank you in advance for your consideration and remain at your disposal should you have any questions.

Sincerely,

Access Now
ARTICLE 19, International
Association of European Journalists, Belgium (AEJ Belgium)
Bits of Freedom, Netherlands
Bolo Bhi, Pakistan
Centre for Democracy and Technology Europe (CDT Europe)
Chaos Computer Club (CCC), Germany
Civil Liberties Union for Europe (Liberties)
Committee to Protect Journalists (CPJ)
Community Media Forum Europe (CMFE)
Council of Bars and Law Societies of Europe (CCBE)
Cryptee, Estonia
D3 – Defesa dos DIreitos Digitais, Portugal
Danes je nov dan, Slovenia
Datenpunks, Germany
Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany
Deutscher Anwaltverein (German Bar Association)
Digital Rights Ireland
Digitale Gesellschaft, Germany
Digitale Gesellschaft, Switzerland
eco – Verband der Internetwirtschaft e.V.
Electronic Frontier Foundation (EFF), International
Electronic Privacy Information Center (EPIC), United States of America
Element
Epicenter.works – for digital rights, Austria
Eurocadres
EuroISPA – The European Association of Internet Services Providers
European Broadcasting Union (EBU)
European Digital Rights (EDRi)
European Federation of Journalists (EFJ)
European Magazine Media Association (EMMA)
European Newspaper Publishers' Association (ENPA)
European Publishers Council (EPC)
Global Forum for Media Development (GFMD)
Global Network Initiative (GNI)
Heartland Initiative
IFEX
Initiative für Netzfreiheit, Austria
IT-Pol, Denmark
La Quadrature du Net, France

Ligue des droits humains, Belgium
Mailfence, Belgium
Malta Information Technology Law Association (MITLA)
News Media Europe (NME)
Nextcloud GmbH, Germany
Panoptykon Foundation, Poland
Politiscope, Croatia
Privacy International
Proton, Switzerland
SHARE Foundation, Serbia
South East Europe Media Organisation (SEEMO)
Statewatch, International
Tech Global Institute
Tuta Mail, Germany
Wikimedia Foundation