Open Letter: Defend encryption and put human rights at the core of cyber-crime related policies: A civil society response to the leaked notes of the EU-US Senior Officials Meeting on Justice and Home Affairs on 16 and 17 March

Dear President von der Leyen, Prime Minister Ulf Kristersson,
Executive Vice-President Margrethe Vestager,

cc Commissioner Thierry Breton,
cc Commissioner Didier Reynders,

The undersigned organisations work to defend human rights in the digital era. We are writing this joint letter as we are **deeply concerned with with the disregard for international human rights standards and the planned attacks against encryption** in the leaked notes from the EU-US Senior Officials Meeting on Justice and Home Affairs, held in Stockholm on 16 and 17 March.

Firstly, we are concerned with the flagrant attacks on the privacy and confidentiality of communications, and in particular on the use of encryption. The document states that the EU and US delegations jointly agreed on the need to promote in public discourse **'law enforcement's legitimacy to investigate' encrypted communications and on 'the need to mirror privacy by design with lawful access by design'**. People living in the US and Europe, businesses, and governments rely on encryption to safeguard their data and resources. As the UN High Commissioner for Human Rights has stated, encryption is a key enabler of privacy and security online and is essential to safeguarding rights including the rights to freedom of opinion and expression, freedom of association and peacefully assembly, security, health and non-discrimination. Our long-term engagement in this field tells us that **'lawful access by design' could only lead to a systemic weakening of encryption worldwide, making everyone unsafe and vulnerable to unlawful access**. Other concerns raised by the document are that 'data retention and data processing (...) [are] identified as areas of focus' by the US delegation. The EU has now a rich body of case-law posing clear limits against general and indiscriminate data retention and strict requirements for public authority access to personal data. Any attempt to circumvent these legal obligations would be in violation of people's fundamental rights.

Secondly, we note that data protection is rightly a key consideration in the EU-US cooperation frameworks on cross-border access to data and information sharing. However, in violation of this commitment, we stress that international agreements in this area often accommodate bad human rights practices and turn into a race to the bottom in terms of data protection requirements. For example, **while the US and EU praise the Budapest Convention and its Second Additional Protocol as a 'gold standard', civil society worldwide, data protection authorities and lawyers' associations have repeatedly criticised**

its lack of adequate fundamental rights protections.[1] **It is even doubtful that this instrument is compatible with EU Treaties**.[2] It is therefore concerning that it could be used as benchmark in the context of the UN cyber-crime convention, which would be signed and ratified by States that do not necessarily have robust data protection frameworks, not to mention adequate human rights records.

Thirdly, **we note with concern the implementation of several initiatives between the EU and the US regarding sharing of "battlefield" or military-produced evidence for use in criminal investigations and immigration proceedings, such as processing of visa and asylum applications**. There is a risk that Europol becomes a data-laundering service for sensitive biometric data which could not be lawfully collected under EU law. The opaque data collection by the US and subsequent transfer to the EU is likely to deprive vulnerable individuals, in particular asylum-seekers and undocumented people, of critical fundamental rights protections and access to effective remedies. We are also deeply concerned that biometric data are about to be transferred under the Enhanced Border Security Partnership (EBSP) before the data-exchange agreement between the EU and the US has even been completed and subjected to the democratic scrutiny of the European Parliament and national parliaments. This is all the more important as the existing data protection framework for EU-US law enforcement cooperation (Umbrella Agreement) would certainly not pass the scrutiny of the Court of Justice of the European Union applied in Schrems and Schrems II cases.[3] At present, there is very little publicly-available information about the EBSP, and most of it comes from leaked documents which very worryingly suggest that biometric data could be shared on a massive scale.[4]

The undersigned organisations call the US government, the EU Member States and the European Commission to:

- **defend and promote encryption, privacy and confidentiality of communications as cornerstones of democracies in the digital age** and abandon any attempt to undermine encryption by promoting client-side scanning, key escrows or other

---

1 Electronic Frontier Foundation, 'EFF to Council of Europe: Flawed Cross Border Police Surveillance Treaty Needs Fixing—Here Are Our Recommendations to Strengthen Privacy and Data Protections Across the World' (20 August 2021) https://www.eff.org/deeplinks/2021/08/eff-council-europe-flawed-cross-border-police-surveillance-treaty-needs-fixing
EDRi and al., '6th round of consultation on the Cybercrime Protocol and civil society participation' (2 May 2021) https://edri.org/wp-content/uploads/2021/05/20210420_LetterCoECyberCrimeProtocol_6thRound.pdf
European Data Protection Board (EDPB), 'EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime' (4 May 2021) https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-contribution-6th-round-consultations-draft-second_en
Council of Bars and Law Societies of Europe (CCBE), 'CCBE comments on the Draft 2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence' (12 April 2021) https://rm.coe.int/0900001680a25786

2 EDRi, 'Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention Why is the opinion of the Court of Justice of the European Union necessary?' (13 April 2022) https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf

3 Laura Drechsler, 'The Achilles Heel of EU Data Protection in a Law Enforcement Context: International Transfers Under Appropriate Safeguards in the Law Enforcement Directive' (31 January 2020). Huygens Editorial 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3664125

4 Statewatch, 'USA offers foreign states access to 1.1 billion biometric "encounters" in return for reciprocal database access' (22 July 2022) https://www.statewatch.org/news/2022/july/usa-offers-foreign-states-access-to-1-1-billion-biometric-encounters-in-return-for-reciprocal-database-access/

forms of unlawful or mass interception of private communications or other interferences that violate the Charter of Fundamental Rights;

- **ensure in current and future legislation and international agreements that privacy by design and by default are legal obligations** that are only limited by necessary and proportionate interferences as required by international human rights law;
- **ensure that the EU-US e-evidence agreement upholds existing international human rights protections in both EU and US law** while addressing conflict of law issues stemming from unilateral measures for cross-border access to data in the EU and the US that currently create considerable legal uncertainty for individuals and service providers; In essence, no state should access data in any other state without the knowledge and consent of the target state, and never in breach of the law (including, where applicable, EU law) in the target state;
- **review and adapt the Umbrella Agreement for the bilateral e-evidence cooperation framework as well as data transfers between EU Member States and the US** under the Second Additional Protocol of the Budapest Convention to ensure they comply with European Convention of Human Rights (ECHR) and the European Charter of Fundamental Rights standards; and
- **ensure that the UN Cybercrime Treaty's criminalisation scope is limited to a narrow set of cyber-dependent crimes,** that it includes strong procedural safeguards in legal assistance and that it does not require the undermining of encrypted systems

Signed by:

European Digital Rights (EDRi)
ApTi (Romania)
Bits of Freedom (Netherlands)
Centre for Democracy and Technology Europe (CDT Europe) (Europe)
Chaos Computer Club (Germany)
Digitalcourage (Germany)
Digitale Gesellschaft (Germany)
Homo Digitalis (Greece)
Statewatch (international)