European Digital Rights

Joint Civil Society written submission to the High Level Group "Going Dark"

Joint Civil Society written submission to the High Level Group "Going Dark" 1

This paper gathers the input of the following civil society organisations:

European Digital Rights (EDRi) is a network of 50+ NGOs across Europe and beyond that defend and promote human rights in the digital era.

IT-Pol Denmark (member of EDRi) works to promote privacy and freedom in the information society and focuses on the interplay of technology, law and politics.

Privacy International (member of EDRi) is UK based nonprofit that campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change.

Statewatch (member of EDRi) produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns on civil liberties, human rights and democratic standards in Europe since 1991.

Introduction

This submission aims to present the viewpoint of digital rights organisations to the High Level Group (HLG) on "access to data for effective law enforcement". The written contribution supplements our oral interventions on 20 February 2024.

Although we welcome the initiative of the HLG to consult civil society and the general public, ad-hoc public consultation meetings cannot amount to a genuinely inclusive and participatory process that meets the EU standards of transparency, fairness and accountability. In addition we note that, to date, we still have not

received any official reply from the HLG co-chairs to our letter sent on 15 January 2024 calling the HLG for greater transparency and participation of all stakeholders.[1]

We would like to stress that this written contribution does not amount to a tacit agreement with the objectives of the HLG. We believe the political agenda of the HLG is narrowly focused on law enforcement interests, in particular access to data, without proper regard for the fundamental rights implications of the suggested or implied solutions. This one-sided approach might lead to inadequate policy recommendations, with high risks of producing poorly-designed and non-future-proof legislation such as the Data Retention Directive annulled by the Court of Justice in 2014 and the Commission's current CSA Regulation proposal.[2]

The written contribution is based on the limited material published by the HLG on its website as well as research and position papers by the undersigned civil society organisations, notably the EDRi position paper on 'State access to encrypted data'.[3] Besides general comments on the fundamental rights at stake and other issues (e.g. technological aspects), we will duly address the specific topics chosen by the HLG for its three working groups (WG1-WG3) and the sessions of the public consultation meeting on 20 February 2024 (data at rest in a user's device, data at rest in a provider's system, and data in transit).

We wish to point out, however, that these topics are narrowly focused on law enforcement investigative interests and, besides the insufficient regard for fundamental rights implications mentioned above, generally fail to consider security in the online sphere from a broader societal perspective, where encryption plays an indispensable role in protecting individuals and organisations, including governments and their services, against a number of threats like cybercriminals and malicious state actors.

In the background document for the first plenary meeting of the HLG, access to data is identified as a challenge for law enforcement. Three reasons for data not being available are then identified: data is not stored/retained, data is encrypted and data is not released by the service provider.[4] This problem definition forms the basis for the work by the HLG and its three working groups. The problem is presented as if increased data access in itself is an objective of general interest, and that the current situation systematically prevents

---

1 EDRi, "Call to the High Level Group on Access to Data for Effective Law Enforcement for greater transparency and participation of all stakeholders", 10 January 2024 https://edri.org/wp-content/uploads/2024/01/Civil-Society-Letter-to-HLG-Going-Dark-on-Transparency-and-Participation.pdf

2 Under the guise of creating 'an obligation of result not of means', the CSA Regulation proposal effectively mandates backdoors in end-to-end encrypted (E2EE) communications services, while leaving the technical implementation aspects, and the responsibility for substantially weakening the security of communications services for all users, entirely to private companies. European Commission, Questions and Answers –New rules to fight child sexual abuse, 11 May 2022 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2977

3 EDRi, Position Paper: State access to encrypted data, 21 October 2022 https://edri.org/our-work/breaking-encryption-will-doom-our-freedoms-and-rights/

4 Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement, 19 June 2023 https://home-affairs.ec.europa.eu/document/download/1d562250-65e3-46fb-a2d7-c64892699c92_en?filename=HLG-background-document-19062023.pdf (page 3)

law enforcement authorities from carrying out their tasks. The background document for the second plenary meeting highlights the difficulties in providing statistics which could quantify the importance of lawful access to data.[5] However, EDRi has repeatedly pointed out that this failure by EU institutions and Member States' authorities to provide evidence about the marginal benefits of access to electronic data compared to less intrusive alternatives leads to legislative proposals which do not satisfy the test of necessity.[6] The provision of evidence is critical for assessing the validity of the assumptions, objectives and recommendations of the HLG, but this question is completely brushed away by the HLG.

In the discussions on data retention for the past two decades, governments have claimed that absence of general and indiscriminate data retention (mass surveillance) has a negative effect on law enforcement's ability to combat crime. However, evidence to support this claim has never been presented. There is no measurable effect from data retention on crime rates or crime clearance rates in EU Member States.[7]

With the pervasive use of online services and smartphones, and the predominant business model of surveillance capitalism which leads to massive data collection for commercial purposes (e.g. behavioural advertising and training large AI models), law enforcement is literally enjoying a golden age of surveillance with access to more data about European citizens than ever before. Before mobile phones became ubiquitous, people didn't carry electronic devices which allow law enforcement to track the physical movement, social networks, preferences and habits of everyone. This, by itself, should call into question the necessity of proposals for general and indiscriminate data retention or restrictions on encryption. Such measures constitute particularly serious interferences with the fundamental right to privacy and data protection, as well as other fundamental rights, and they generally fail to meet the legal requirements for necessity and proportionality in Article 52(1) of the Charter of Fundamental Rights.

The background document for the second plenary identifies "the current state of the public discourse concerning privacy and security, which are at times erroneously contrasted" as a factor which has negatively affected the development of legislation on law enforcement access to data. From our understanding of what this refers to, blaming voices in the public sphere that advocate for the safety, privacy and free expression of all users globally, is deeply concerning. We agree, however, that the contrast between privacy and security is wrong given that both people's privacy and security are attacked when digital infrastructures are undermined. Enjoying our right to privacy online allows us to do our jobs, organise, exercise our free expression and hold power to

5 "Despite requests to this end, it appears unfeasible for law enforcement authorities to classify the criminal case types that are more or less reliant on access to data to be solved, as well as the categories of data which are necessary to investigate and prosecute criminal offences. National experts highlighted the difficulties faced in providing statistics which could quantify the importance of lawful access to data for successfully investigating and prosecuting crime, regardless of the type of offence suspected or the type of data required", Input to the second plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement, 21 November 2023 https://home-affairs.ec.europa.eu/document/download/05963640-de76-4218-82cd-e5d4d88ddf96_en?filename=HLG-background-document-21112023.pdf (page 2)

6 EDRi, Data Retention Revisited, 2020 https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

7 EPRS, General data retention / effects on crime, 5 October 2020 available at: https://www.patrick-breyer.de/en/study-data-retention-has-no-impact-on-crime/?lang=en

account while remaining safe from arbitrary intrusion, persecution or repression.

In a democracy, law enforcement authorities will never be granted unfettered surveillance powers, and all intrusive investigative measures must be subjected to public scrutiny for an assessment of their necessity and proportionality. At the same time, the HLG deliberately attempts to reframe the public debate in a highly misleading way. It does so by redefining 'security by design' in the HLG scoping paper as the combination of 'access by design' and 'privacy by design', which can only really be construed as a desire to have law enforcement backdoors everywhere.[8] According to the scoping paper, the HLG will address the issue of fundamental rights from the perspective of victims and potential victims, which is clearly inadequate and incomplete for assessing the fundamental rights impacts of all affected individuals and communities by law enforcement measures on access to data.

This paper is structured according to the HLG proposed sessions at the public consultation meeting on 20 February 2024 (data at rest in a user's device, data at rest in a provider's system, and data in transit).

Access to data at rest in a user's device (WG1)

Working group 1 explores the challenges faced by law enforcement when seeking to access information on smartphones, laptops and other devices (e.g. USB storage) that have been physically seized by law enforcement in the conduct of investigations. The problems identified by WG1 are device (disk) encryption and the use of hardware security models to securely manage the mobile device's decryption keys. As the working group recognises, these elements are now standard features on smartphones and laptops.

Smartphones contain very sensitive information about their owners

The two published background documents for WG1 only deal with the perceived operational challenges of getting access to data on devices that have been seized. There is no analysis of the interferences with fundamental rights when law enforcement extracts personal data from mobile devices, nor is there any consideration of appropriate substantive and procedural safeguards for such access.

Smartphones often contain the most intimate details of our private life. Smartphone apps have access all our communication channels and social media accounts, sensors that may record very private details of our bodies, especially when connected to activity trackers or smartwatches, fine-grained location records, and cameras that we use to collect visual memories of our physical whereabouts, participation in public protests, and interactions with other individuals. The modern smartphone has almost become a digital extension of our body, mind and thoughts. In the words of the European Data Protection Supervisor, "Our smartphones know everything about us: they know our data, they can hear us, they can see us, and they know where we are and who we talk with."[9]

---

8 Council Document 8281/23 (Scoping paper for the High-Level Expert Group on access to data for effective law enforcement) https://data.consilium.europa.eu/doc/document/ST-8281-2023-INIT/en/pdf

9 EDPS, Preliminary Remarks on Modern Spyware, 15 February 2022 https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

Law enforcement is, of course, taking advantages of this treasure trove of information about individuals which did not exist 15 years ago. Information extracted from seized smartphones is increasingly used as evidence in investigations or to supposedly verify the veracity of asylum applications.[10] Private companies sell specialised equipment to law enforcement to facilitate and streamline the data extraction. These data extraction tools are becoming widely used, also in local police stations to prosecute any and all crimes, even petty ones.[11]

Data extraction from a mobile device is particularly problematic because there is no technical way to limit law enforcement access to a particular piece of information on the device. If law enforcement authorities are successful in unlocking the mobile device, either by brute-forcing access or by persuading the owner to unlock it, they get physical access to everything on the device, just like the owner would, except for the rare situation where certain apps are protected with separate passwords.

Legal protection against law enforcement access to mobile devices

The legal protection against this potentially uncontrolled data extraction from mobile devices is grossly ineffective. In many Member States, the ordinary rules for police gathering of evidence apply, and the smartphone is simply one of many objects that can be seized in the conduct of investigations. Legal protections that apply when e.g. telephone calls are intercepted, may not apply when private communications are extracted from the device storage. Furthermore, even when legal protections exist, they tend to not be respected in practice by authorities. In 2023 the German Federal Administrative Court had to stop the quasi-systematic extraction of mobile phone data by the Federal Office for Migration and Refugees (BAMF) to register and process asylum claims. The Court ruled that the routine practice of requesting asylum seekers to unlock their mobile phone and the subsequent data analysis was disproportionate and illegal.[12]

Whether EU law restricts law enforcement access to personal data stored on smartphones is subject to a case (C-548/21) currently pending before the Court of Justice. The Advocate General (AG) dismisses the assumption of the referring Austrian Court that the ePrivacy Directive 2002/58 applies.[13] Based on interpreting the Law Enforcement Directive (LED), the AG also rejects that law enforcement access to data on a mobile device should be limited to investigations of serious crime, and instead proposes that it "must be justified in each case and must be limited to what is strictly necessary and proportionate according to the nature of the crim-

10 Gesellschaft für Freiheitsrechte, Invading Refugees' Phones: Digital Forms of Migration Control, February 2020 https://freiheitsrechte.org/uploads/publications/Digital/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control-Gesellschaft_fuer_Freiheitsrechte_2019.pdf

11 Reporterre, Nous avons visité Milipol, le salon de la répression, 21 November 2019 https://reporterre.net/Nous-avons-visite-Milipol-le-salon-de-la-repression

12 Francesca Palmiotto and Derya Ozkul, ""Like Handing My Whole Life Over" The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures", 28 February 2023 https://verfassungsblog.de/like-handing-my-whole-life-over/ Like the authors in this article, we also believe the German Federal Administrative Court missed the opportunity to assess data protection aspects, notably the principles enshrined in the GDPR, in this case.

13 AG Opinion in case C.548/21 Bezirkshauptmannschaft Landeck https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CC0548

inal offences under investigation and of the personal data to which access is sought." National law must provide procedural rules, and prior authorisation from a court or independent administrative authority is required when the personal data extracted make it possible to obtain a detailed picture of a person's private life.

The proposal of the AG will leave a lot of discretion to Member States' police authorities who will be naturally inclined to believe that their evidence collection is done in a proportionate way. There must be a general presumption that data stored on a mobile device make it possible to obtain a detailed profile of the owner, but by not requiring a court order in all cases, the AG again leaves considerable discretion to Member States. Moreover, the AG Opinion does not address how a court authorisation can effectively ensure that the extracted information is actually limited to what is strictly necessary and proportionate.

In our opinion, safeguards and protection against abuse could be improved if the data extraction was performed by an independent body whose sole role in the investigation is to ensure that only information from the mobile device expressly allowed by the court authorisation is turned over to the police, and that anything else is immediately deleted.[14] This is critical to prevent fishing expeditions. If the police is allowed to indiscriminately search the device (a common practice today), no safeguards are adequate or effective for protecting the fundamental rights of the device owner. The police could, for example, use the pretext of prosecuting minor offences (e.g. use of drugs) to seize and search a phone and in reality look for evidence of guilt of more serious crime but for which no reasonable grounds can be presented to justify a search order.

If the data extraction is performed by an independent body with the procedural guarantees outlined above, persons suspected of a criminal offence may even be willing to unlock their mobile device in order to be cleared of suspicion. The refusal to do so should, of course, not affect the presumption of innocence and the prohibition against self-incrimination. We would like to stress that we firmly oppose the use of coercion as an adequate alternative in order to access data on mobile devices as it constitutes a particularly serious infringement of privacy and the right not to self-incriminate, and even potentially the prohibition of torture and other inhuman or degrading treatments.

These safeguards do not exist today in EU Member States. If a mobile device is seized, only effective encryption that cannot be circumvented will protect against uncontrolled law enforcement access. These technical measures also protect against unlawful access to the information on the device if it is stolen or lost. Indeed, for many individuals that may be the primary concern, as they don't expect to become involved in a law enforcement investigation. However, an effective technical protection against unlawful access if a device is lost will also, by construction, protect against lawful access by law enforcement.

---

14 Safeguards along these lines can be found in the New Mexico state Electronic Communications Privacy Act. When issuing a search warrant for data extraction from a mobile device, the court may appoint a special master charged with ensuring that only the information necessary to achieve the objective of the warrant is produced or accessed. See https://nmlegis.gov/Sessions/19%20Regular/final/SB0199.pdf and the report by Upturn, Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones, October 2020 https://www.upturn.org/work/mass-extraction/ which pointed our attention to the New Mexico law.

Device backdoors will recklessly undermine the security of everyone

The working group is predominately concerned with situations, where the combination of device encryption and hardware security models to protect decryption keys against brute-force access (e.g. rate-limiting password or PIN attempts) makes it impossible to extract data from the device, or where such decryption takes a very long time (24 months is mentioned).

No statistical data is provided to support these concerns. Vendors of digital forensic solutions such as Cellebrite, MSAB and Grayshift regularly claim on their websites that they are able to extract data from a number of different smartphone models. It is our understanding that the digital forensics vendors gather information about security vulnerabilities on mobile devices and use that to brute-force access (where possible). Moreover, many individuals use easily guessable passwords or PIN codes (such as their birth date as PIN code), where rate-limiting the number of password guesses in a hardware security module provides no protection. In a comprehensive study of US law enforcement from October 2020, the non-profit organisation Upturn reports that "[their] findings suggest that today's mobile device forensic tools can extract data from most phones."[15] Lastly, one of the operational challenges identified by the HLG is that Member States refrain from sharing digital forensics tools and decryption capabilities, either due to a lack of trust or national security concerns.[16]

In the second background document for WG1, possible solutions are outlined. Besides increased digital forensic cooperation and capacity building between Member States, the document outlines "potential avenues" for engagement and cooperation with industry and legislative approaches to enable lawful access for law enforcement to data at rest in devices and applications. The description of these solutions match the one of encryption backdoors, either through voluntary cooperation with device manufacturers and standardisation bodies or mandated through legislation.

Mobile device manufacturers have invested considerable resources in improving the security of their devices, not the least due to demands from privacy-conscious customers as well as regulatory authorities, especially from the cybersecurity and data protection fields. On-device encryption can protect against personal data breaches in case mobile devices are lost. Indeed, EU data protection authorities have issued fines in data breach cases to data controllers who failed to activate disk encryption on their mobile devices.[17] Against this backdrop, it seems very unlikely that mobile device manufacturers will even consider voluntarily weakening the security of their devices with backdoors for law enforcement access. It is technically impossible for them to design an encryption backdoor for a specific actor without creating a substantial risk that the same backdoor will be abused by others actors.

---

15 Upturn, Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones, October 2020 https://www.upturn.org/work/mass-extraction/

16 Background document for the second plenary of the HLG, page 5.

17 See e.g. European Data Protection Board, Polish SA fines controller EUR 2200 for failure to implement appropriate security measures, 9 June 2023 https://edpb.europa.eu/news/national-news/2023/polish-sa-fines-controller-eur-2200-failure-implement-appropriate-security_en and Datatilsynet, Hørsholm Municipality fined DKK 50,000. 29 September 2022 https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/hoersholm-kommune-idoemt-boede-paa-50000-kr

Even though the purpose is targeted lawful access (on devices that have been lawfully seized), the suggested measures will result in a general and indiscriminate interference with the fundamental rights to privacy and data security as virtually all users will see their own device security weakened. In a recent judgment from the European Court of Human Rights (case 33696/19, Podchasov v Russia), this weakening of security is rightfully regarded as a disproportionate interference with fundamental rights.

Furthermore, mandatory backdoors would undermine EU's cybersecurity policies and legitimate interests. A high level of cybersecurity is difficultly achieved in practice, partly because current commercial and political interests in stockpiling security vulnerabilities contradict its very objectives. The last thing that is needed, from a broader societal perspective, is legislation imposing security vulnerabilities just waiting to be abused by malicious actors.

Access to data at rest in a provider's system (WG2)

The working group focuses on the retention of metadata by providers of electronic communications services. This topic has been discussed in several Council working groups since the beginning 2017, when Member States started to consider the implications of the Tele2 judgment of the Court of Justice of the European Union from 21 December 2016. WG2 seems largely to be a continuation of that work.

The essence of the discussions since 2017, according to the Council documents that have been made publicly available, is that most Member States want a general and indiscriminate obligation for service providers to retain communications metadata. However, the ePrivacy Directive interpreted in light of the Charter prohibits general and indiscriminate retention obligations for the purpose of combatting serious crime, with some limited exceptions (IP address assigned to the source of an internet connection and subscriber identity data).

Data retention has become a rule of law crisis for Europe

Council working groups since 2017 and now WG2 have looked for 'a way forward' that would somehow allow Member States to maintain their data retention laws that originally transposed the Data Retention Directive. Ten years after the annulment of that directive in April 2014, the national data retention laws are still in place in the majority of Member States, despite a number of subsequent CJEU rulings on essentially the same question: general and indiscriminate data retention for combatting serious crime is contrary to EU primary law. Nonetheless, Member States continue to send new data retention cases to Luxembourg and pleading for the Court to revise its case law. After the CJEU clarified in October 2020 that EU law does not preclude a general and indiscriminate retention obligation for source IP addresses for combatting serious crime, Member States are now trying to convince the CJEU that the retained data should be available for all criminal offences.[18]

In the meantime, while putting political pressure on the CJEU to permit more data retention, Member States ignore the Court's rulings and maintain national data retention laws that clearly violate the fundamental rights to privacy, data protection and freedom of expression (under the current CJEU case law). The Commission has

18 European Law Blog, A complete U-turn in jurisprudence: HADOPI and the future of the CJEU's authority, 4 December 2023 https://europeanlawblog.eu/2023/12/04/a-complete-u-turn-in-jurisprudence-hadopi-and-the-future-of-the-cjeus-authority/

repeatedly refused to start infringement proceedings against Member States with illegal data retention laws.[19] It is not an exaggeration that data retention has become a systemic rule of law crisis in the European Union.[20]

Targeted data retention could be a way forward in compliance with the Court's rulings. However, the criteria for targeted data retention (geographical area and group of persons) as permitted by the CJEU are considered unclear by Member States. From our perspective, it is true that the use of these criteria raises many questions in terms of the respect for a wide range of human rights, including the presumption of innocence and the right to non-discrimination. Although the Court specifies that the factors should be objective and non-discriminatory, the reality of police racism and discriminatory law enforcement practices[21] makes us strongly doubt that these requirements are currently achievable.

In reality, governments have done very little to explore this option in accordance with the guidance provided by the CJEU. Belgium and Denmark have adopted legislation on targeted data retention, but the measures in both countries are in fact general and indiscriminate data retention in disguise.[22] The thresholds selected in both laws are so low that they are rendered meaningless as almost the entire the population is covered by the data retention obligation. As a result, the practical implementation of the supposedly targeted data retention regimes would literally amount to a general and indiscriminate retention, which is highly likely to be overturned by the CJEU.

The "avenues to explore" in the second background document for WG2, the background document for the second plenary, as well as presentations by Germany, Spain, Italy and Slovakia which have been released through a freedom of information request by Patrick Breyer[23] (with some redactions), taken together suggest that the discussions in WG2 are going in circles around the same questions which have been on the table in various Council working groups since 2017.

Exploring legislation on data retention compatible with the CJEU case law means repealing existing data retention regimes in most Member States (except the handful of Member States, where national courts have invalidated the data retention law and no new data retention was adopted by the legislator).

19 EDRi, "European Commission will "monitor" existing EU data retention laws", 29 July 2015 https://edri.org/our-work/european-commission-will-monitor-existing-eu-data-retention-laws/
EDRi, "Europe's Data Retention Saga and its Risks for Digital Rights", 2 August 2021 https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/

20 POLITICO, Lawless Europe, July 2022 https://www.politico.eu/special-report/lawless-europe/

21 ENAR, "Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe", 5 November 2019 https://www.enar-eu.org/wp-content/uploads/data-driven-profiling-web-final.pdf

22 EDRi, "New Belgian data retention law: a European blueprint?", 17 November 2021 https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/
Jesper Lund, "The new Danish data retention law: attempts to make it legal failed after just six days", 15 June 2022 https://itpol.dk/articles/new-Danish-data-retention-law-2022

23 FragDenStat, June and November Meetings of the HLEG on access to data for effective law enforcement (FOI request) https://fragdenstaat.de/anfrage/june-and-november-meetings-of-the-hleg-on-access-to-data-for-effective-law-enforcement/

Data retention extended to over the top (OTT) services

The background documents reveal an interest in extending data retention laws to OTT (over the top) providers, which since December 2020 are part of the ePrivacy data protection regime as providers of number-independent electronic communications services. Although the CJEU has not ruled on data retention for such providers, it must be assumed by analogy that a general and indiscriminate retention obligation for all EU users is prohibited by the ePrivacy Directive and the Charter. Only targeted retention can be compatible with EU law, at least insofar as the retention obligation applies to metadata which allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, e.g. their location and physical movement, their social relationships and their social environments.[24] This includes any metadata about actual private communications (sender, recipient, time of communication) and any location data collected by the service provider.

Most number-independent services are offered globally through the internet (OTT) by companies with a main establishment outside the European Union. The providers may not technically be able to comply with a data retention obligations for some of their European users. They certainly cannot be expected to introduce a global data retention scheme through their terms of service in order to comply with national law in a given EU Member State.

The background documents point out that some OTT providers retain no data at all. This is to be expected given the increased global focus on privacy, the advantages of anonymous communications, and the risks associated with storing personal data (e.g. behavioural profiling and data breaches). These are the same drivers that lead people to prefer secure end-to-end encryption (E2EE) communications services over cleartext services, where their private communications and associated metadata can be monitored by private companies and state actors.

Some E2EE communication services apply concepts such as 'sealed sender' that technically prevents even the service provider from monitoring who is communicating with whom. This technical design supports key principles in EU data protection law, notably data protection by design in Article 25 of the GDPR and the main rule in the ePrivacy Directive that users' communications and data relating thereto will remain anonymous and may not be recorded.[25] However, this also means that a data retention obligation for metadata is technically impossible due to the design of service. In this connection, it should be recalled that the scope of the Data Retention Directive was traffic data generated or processed by the provider, which refers to data that is actually accessible to the provider.[26]

In summary, while a data retention obligation in compliance with the case law of the CJEU could, in principle, be extended to number-independent services (OTT providers), there will be a number of legal, jurisdictional and technical obstacles that are likely to render the proposal infeasible in practice.

24 Cf. Tele2 judgment (joined cases C-203/15 and C-698/15), para. 99

25 Cf. para. 109 of La Quadrature du Net and Others (joined cases C-511/18, C-512/18 and C-520/18)

26 Recital 13 of the Data Retention Directive 2016/24/EC (annulled)

As civil society organisations, we seriously question the necessity of additional data retention obligations for OTT services when most of these services already collect a substantial amount of personal data for their commercial purposes, especially the predominant Big Tech services. The e-Evidence Regulation will from August 2026 enable law enforcement authorities in Member States to issue cross-border production and preservation orders directly to service providers offering services in the EU.

As regards the limited number of privacy-focused services with E2EE and no metadata collection for commercial purposes, they are also likely to employ anonymity-by-design technologies that make metadata collection impossible. Pressuring security-focused providers of electronic communications services into weakening the security of their service would undermine the right to privacy and data protection as well as the security of all their users. Being able to develop, offer and choose trustworthy communication systems is essential in democratic societies. Most likely, security-focused providers established outside the EU would simply refuse to do so, similar to their refusal to comply with national laws requiring encryption backdoors.

Real time access to data in transit (WG3)

As emphasised in EDRi's position paper 'A Safe Internet for All', measures which aim to circumvent the security and confidentiality of encrypted communications or other encrypted digital services undermine the essential purpose of that encryption, and cannot be accepted in a democratic society.[27] This applies to any measures that are applied without specific warranted suspicion, or which would undermine the security or integrity of the encrypted communications in general (rather than only of the specific person under investigation).

For the purpose of the discussion on real time access to data in transit, we pose the definition of "encryption backdoors" as any intentionally built-in mechanism used to circumvent a system's security measures in order to gain access to that system or its data and that undermine the principle that only the sender and recipient of communications can read them. In that sense, it does not matter what data is collected and for which period of time.

Lawful and unlawful interception for traditional telephone services

With traditional telephone services, law enforcement can intercept real-time voice and text message (SMS) communications with compelled assistance from the service provider. Member States' national laws set out requirements for the technical assistance from telecommunications ("telecoms") operators ("legal interception"). The interception takes places in the central systems of the operator while the communication is in transit between the sender and the recipient. This is technically possible because traditional telephone services are not end-to-end encrypted (E2EE) between the sender and recipient. Voice and text message content are generally transmitted through telecom systems such as SS7 without any encryption at all.

Due to the lack of encryption, traditional telephone communications can be intercepted by other parties than law enforcement authorities. The Snowden documents revealed that intelligence agencies are conducting mass surveillance for alleged national security reasons by tapping fibre optic cables. Moreover, the legal inter-

27 EDRi, "A Safe Internet For All", October 2022 https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

ception systems operated by telecom operators can be compromised and abused by malicious actors. The Greek wiretapping scandal of 2004-05 illustrated well the risks of exploitation of lawful interception systems by unauthorised third parties.[28] Communications interception by criminals continues to be a common threat today, for example for stalking, blackmail or identity theft.

In today's cybersecurity threat landscape, traditional telephone services must be regarded as insecure and highly vulnerable to unlawful surveillance. Indeed, the public authority responsible for cybersecurity in Denmark recommends to use E2EE (OTT) communications services such as the encrypted Signal app because traditional telephone services are vulnerable to surveillance.[29] The European Commission itself has ordered its staff to use Signal in order to increase the security of its communications.[30] The advice is meant for government officials and civil servants, but the surveillance threat analysis and the need to protect confidentiality of communications applies to everyone. Throughout the world, the work of journalists and human rights defenders is increasingly being criminalised. Encryption protects their work against unlawful surveillance.

The smartphone allows people to use secure E2EE communications services instead of insecure telephone calls and SMS. Considering the threat situation outlined above, as well as the additional features offered by OTT communications services, it is only logical that interpersonal communications are rapidly moving from traditional telephone services to OTT apps. Not all OTT apps offer E2EE communications, but this service becomes more and more mainstream and even expected.[31] E2EE is probably the most effective way to protect our electronic data and offers the best security for individuals. It protects against commercial surveillance by the service provider, unlawful surveillance by governments and cyberattacks against the provider's server infrastructure (without E2EE, the attacker could gain access to the content of the communications).

Lawful interception for E2EE communication services

The traditional lawful interception model with compelled assistance from the service provider is not possible for E2EE communication services. The service provider only has access to encrypted communications content and cannot respond to an interception order (for the plaintext content), even if such an order could hypothetically be issued under the national law of a Member State.

We would like to stress that this is not a new topic of discussion – it has been going on since the start of the 1990s (sometimes referred to as the "crypto wars"). To succinctly summarise a 30-year long public discussion, the service provider can only respond to targeted lawful interception orders by building a backdoor for every

28 IEEE Spectrum, The Athens Affair, 29 June 2007 https://spectrum.ieee.org/the-athens-affair

29 Centre for Cybersecurity, Handbook on security for mobile devices, February 2023 https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/CFCS-haandbog-i-sikkerhed-for-mobile-enheder.pdf

30 POLITICO, "EU Commission to staff: Switch to Signal messaging app" 20 February 2020 https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/

31 Even Meta, whose business model relies on the monetisation of mass amounts of illegally collected personal data for advertising purposes, has started rolling out E2EE by default for all personal chats and calls on Messenger and Facebook. https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/

user, which if activated would allow the service provider to break the technical promise of end-to-end encryption. This backdoor can, and will, be abused by various malicious actors. There is general agreement among scientific researchers and cybersecurity practitioners that it is simply not technically possible to build a backdoor which will only be used by "the good guys". This is not a theoretical conjecture: in cases where backdoors have actually been built into systems, they have generally been exploited by unintended (malicious) actors, e.g. cybercriminals or foreign intelligence services.

In other words, an encryption backdoor to allow targeted surveillance by law enforcement comes at the heavy price of undermining the cybersecurity of all individuals and making them vulnerable to unlawful surveillance and other abuse. Civil society organisations and others have long argued that mandatory encryption backdoors constitute a general and indiscriminate interference with the fundamental rights to privacy, data protection and data security which is disproportionate. On 13 February 2024, the European Court of Human Rights delivered a landmark ruling which confirmed that mandatory encryption backdoors are a violation of Article 8 of the European Convention on Human Rights on the right to respect for private and family life.

The problems identified by the HLG lack nuance

The background document for the second plenary recalls earlier European Council conclusions to safeguard the benefits that E2EE bring for the protection of privacy, data and communication, while at the same time highlighting that effective access to electronic evidence is essential to combatting crime. Under the German Council presidency in 2020, the principle "security through encryption and security despite encryption" was put forward. These policy statements broadly fail to recognise that it is technically impossible to build secure, end-to-end encrypted systems for everyone and have targeted access to the same encrypted data by law enforcement. The fact that doing both is technically impossible may be seen as a dilemma for some policymakers.

More broadly, the framing of encryption as impeding law enforcement work lacks nuance and balance. It overlooks the proven fact that encryption is a vital human rights tool, with organisations across the world emphasising that the security of people's private lives frequently relies on the use of end-to-end encryption.[32] The UN High Commissioner for Human Rights, for example, has emphasised the important role of E2E encrypted services for civilians trying to protect themselves and their families following the Russian invasion of Ukraine in 2022.[33] Since undermining the security of everyone is an unacceptable policy option, there is really only one solution for society: recognise that the benefits of having security for everyone significantly outweigh the occasional problems for law enforcement.

From the background documents published by the HLG, it does not appear that the HLG has come to this realisation or even agrees with it. Working group 3 seems to be operating under the assumption that it is possible to facilitate access to data by law enforcement without compromising the security of everyone. The avenues to

32 For example: https://www.fightforthefuture.org/news/2022-10-13-make-dms-safe-orgs; https://www.hrw.org/tag/encryption; https://edri.org/take-action/our-campaigns/keep-it-secure/

33 United Nations Office of the High Commissioner for Human Rights, press release, 2022, available at: https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

explore in the second background document for WG3 are reminiscent of the failed proposals we have seen for the past 30 years: backdoors or other types of systemic security vulnerabilities.

The challenges are not mainly about legislation, for example that existing legal interception measures only cover telecom operators, or adapting the European Investigation Order to handle cross-border interception cases. Laws can be changed, but the technical reality about encryption backdoors does not change. As a concrete example, the CSA Regulation proposal from the Commission requires an interception (content detection) capability for all interpersonal communications services, including E2EE ones, and the service provider must design its systems so that interception (detection) is always possible.

Relegating the responsibility to private companies may appear as an attractive solutions for policymakers who do not know how to solve the problem (because no solution exists). However, it is not an acceptable solution because service providers are left with the choices of either undermining the security of their systems for all users or refusing to comply with the legislation requiring backdoors. Since the relevant companies generally offer their services globally, they can be meet with conflicting demands for backdoors from a large number of countries, democratic as well as authoritarian like Russia, Iran and China. Refusing to comply because it is technically impossible is really their only choice. The alternative will be undermining the very foundation upon which the company's business model is based (offering secure systems). There are examples (outside the EU) of national laws demanding encryption backdoors in communications services, but no government has been able to enforce such laws.[34]

"Chat control" or client-side scanning

One method of circumventing the promise of encryption, which is not specifically mentioned in the publicly available documents of the HLG but that has received a lot of attention from EU lawmakers is so-called 'Client-Side Scanning' (CSS). This technique is sometimes framed as a safe and viable alternative to inserting an encryption backdoor for remote access to a device since the scanning technologies used are on-device analysis of data before being encrypted or after being decrypted. However, despite the widespread claim of not interfering with encryption, CSS breaks the whole purpose and function of end-to-end encrypted communication, which is the assurance of confidentiality against the service provider and any unauthorised third party.

As emphasised in the recently updated landmark paper 'Bugs in Our Pockets' from several of the world's leading cyber security experts, CSS would insert a vulnerability into all users' devices.[35] CSS implies that surveillance software is hosted on mobile devices which are often vulnerable to "zero days exploits" (unmitigated software vulnerabilities) and can therefore be abused by malicious actors. The United Nations High

34 With Technical Capability Notices in the 2016 Investigatory Powers Act, UK authorities can issue orders for service providers to redesign their systems so that lawful interception is possible. Australia has a similar legislation. In an op-ed in Financial Times, Ciaran Martin, former chief executive of the UK's National Cyber Security Centre points out that, as far as is publicly known, these powers have never been used. See Financial Times, The UK government has sparked an encryption row over powers it might never use, 10 April 2023 https://www.ft.com/content/96964279-8011-4d46-9b90-69e016d39e7f

35 Abelson et al, 'Bugs in Our Pockets', Journal of Cybersecurity, Volume 10, Issue 1, 2024, available at: https://doi.org/10.1093/cybsec/tyad020

Commissioner for Human Rights explains that "Client-side scanning also opens up new security challenges, making security breaches more likely. The screening process can also be manipulated, making it possible to artificially create false positive or false negative profiles."[36]

For example, children who use an encrypted messaging app to communicate with friends and to let their parents know that they are safe when going to and from school would find their phones more vulnerable to hacking by criminals. This could give the latter access to children's personal information, location data, daily behaviour patterns and other sensitive information, putting them at serious risk.

In the European Commission's expert group assessment of CSS as part of the impact assessment to the EU's draft Child Sexual Abuse Regulation, all options explored are assessed as suffering from serious privacy and security risks (including the resilience to abuse by malicious actors).[37]

Given the serious limitations placed upon the rights to privacy, data protection, free expression and association and other fundamental rights of a very high number of persons entailed by measures like CSS, they cannot be considered lawful, necessary or proportionate in accordance with Article 52(1) of the EU Charter of Fundamental Rights.

At the same time, regardless of whether the proposed method for circumventing or weakening encryption at a general level is CSS, "secure enclaves" or something else entirely, the fundamental human rights arguments about necessity, proportionality and lawfulness remain the same.

Bulk hacking operations like EncroChat and SkyECC

The SkyECC and EncroChat operations are mentioned in several background documents of the HLG as case examples raising new challenges as traditional real time interception are ineffective to access communications content. In the document highlighting the avenues to explore, WG3 indicates its intentions of studying "the conditions for legal certainty when using special techniques to access data on devices remotely (...) based on lessons learnt from EncroChat & SkyECC".

In two joint investigation operations, law enforcement authorities in France, Belgium and the Netherlands obtained access to electronic communications data for a large number of individuals suspected of various crimes. The data was obtained in a general and indiscriminate manner where all users were subjected to bulk hacking (sometimes referred to as "bulk equipment interference"). It was subsequently shared with many other states through Europol.

Those operations are alarming for several reasons, notably (1) they unduly undermined people's fundamental rights such as the rights to privacy and data protection, the rights to a fair trial and to effective judicial protec-

36 United Nations Office of the High Commissioner for Human Rights, press release, 2022, available at: https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

37 Impact Assessment for the CSA Regulation proposal, SWD(2022) 209 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0209

tion, the presumption of innocence and journalistic rights (2) they create a dangerous precedent for policing in Europe. This is why they are currently before the courts in several countries and will no doubt end up being challenged in the European Court of Human Rights.

Right to privacy and data protection: Bulk hacking is an extremely intrusive measure as it gives law enforcement authorities access to a much greater amount of "bulk" data, including very sensitive data, than any other traditional and more targeted investigative tools. In his recent opinion on modern spyware inspired by media investigations into Pegasus, the EDPS questioned whether hacking tools that give access to an unrestricted amount of (past and future) data could be within the scope of EU law as the essence of the right to privacy may be affected. This is a severe encroachment on the privacy of all users of both networks. The use of automated and AI-based tools by the authorities to analyse the captured datasets exacerbates the interference with privacy and data protection rights.

Presumption of innocence: Instead of an individualised suspicion to justify the extremely intrusive measure of government hacking and interception of private communications, the investigative authorities simply assumed that most EncroChat and SkyECC users were criminals. Clearly, these authorities could not reasonably have known this beforehand due to the highly anonymous nature of the networks (which in itself is not illegal). As a letter signed by over one hundred Dutch defence lawyers made explicit: "What happens to users' data that cannot be linked to criminal offences is unknown." The letter warned that: "In criminal cases, [everyone] should even be able to rely on the presumption of innocence: guilt of a criminal offence cannot and should not be assumed until the evidence that might serve that purpose has been rigorously tested."[38] As EncroChat and SkyECC users who had nothing to do with any criminal activity were asked to come forward at some point during the investigation in order to have their data discarded from police consideration and analysis, the principle of the presumption of innocence is completely flipped upside down. Such approach is unlikely to pass the test of the courts. Last year, the European Court of Human Rights condemned the Turkish government for taking a uniform and global approach to the use of the Bylock app, an encrypted messaging service supposedly used by the Gülen movement.[39] 92 769 individuals have been arrested in a case where the use of an encrypted app was turned into a presumption of guilt.[40]

Journalistic rights and professional privilege: The user bases of both networks are also likely to have included journalists, whistleblowers and human rights defenders, all of whom have legitimate needs for strong privacy

38 Bill Goodwin, Dutch lawyers raise human rights concerns over hacked cryptophone data, Computer Weekly (October 2022) https://www.computerweekly.com/news/252526497/Dutch-lawyers-raise-human-rights-concerns-over-hacked-cryptophone-data
Letter available at: https://media.licdn.com/dms/document/media/D4E1FAQHyO5aQ3qvwBQ/feedshare-document-pdf-analyzed/0/1666528452891?e=1709769600&v=beta&t=e1EzhDjzuCV_O82MNHFrYo49bw-zVTrtVtNT62FyZZE (in Dutch)

39 European Court of Human Rights, Case of Yüksel Yalçinkaya v. Türkİye (Application No. 15669/20) Judgment, https://hudoc.echr.coe.int/?i=001-227636

40 According to the Arrested Lawyers initiative, "the government claims that anybody who may have downloaded it is, in fact, a "terrorist." The Arrested Lawyers Initiative, Report on the legal and technical issues around Turkey's malicious ByLock Prosecutions, November 2021, available at: https://arrestedlawyers.org/wp-content/uploads/2021/11/report-bylock-november-2021.pdf

protection. In the aftermath of the EncroChat investigation, it has been revealed that law enforcement authorities gained access to potentially privileged communications between lawyers and their clients, which is in breach of national laws granting special protection to data and communications exchanged between lawyers and their clients or between journalists and their sources.[41]

Right to a fair trial: The claim of "defence secrecy" by the French authorities has left almost all defendants in Europe powerless as they are not able to properly challenge the evidence against them. Prosecuting authorities have been relying on "mutual trust" to oppose any form of disclosure to accused persons. This means that the defence is facing secret evidence: it is impossible to challenge the legality of the investigation technique as well as the accuracy, reliability and authenticity of the data collected; exculpatory evidence that may exist within the hacked data is often out of reach, inaccessible to the defence. Keeping the operation methods confidential severely impaired the fundamental right to a fair trial. In the ByLock case mentioned above, the Strasbourg Court condemned the Turkish state after concluding that the applicant did not have a genuine opportunity to challenge in court the evidence held against him effectively. We also know that accused persons have been coerced into guilty pleas without even going to trial because they are unable to prepare an effective defence, leading potentially to miscarriages of justice.

Furthermore these operations are raising significant concerns as to their legality, the respect of the rule of law and the risk of normalisation of such policing methods in the future.

Jurisdictional overreach: Since the users of EncroChat and SkyECC and their geographical location were largely unknown before initiating the bulk hacking operation, the French and Dutch authorities effectively conducted their investigation on the territories of other Member States without any regard to the domestic rules and safeguards for interception of private communications.

Legal uncertainty and forum shopping: Bulk hacking operations like the EncroChat and SkyECC investigations are not necessarily legal in every Member State. Even in Member States that have provisions for bulk hacking, the legality of an investigation like EncroChat can be highly uncertain. When Europol analyses and "distributes" communications data, at least some Member States' authorities may receive information that they could never have obtained legally in a domestic investigation. This affects the foreseeability and clarity of the application of domestic law if people can have their rights interfered with by foreign authorities, bypassing domestic legal protections and affording no recourse.

Normalisation of data mining: The framing of EncroChat and SkyECC operations as law enforcement successes risks normalising the deployment of fishing expeditions combined with the use of AI-based data mining tools to analyse the large amounts of data captured. It has actually already offered the justification to reform Europol's mandate in order to allow the agency to circumvent its own rules when it 'needs' to process data

41 Investigative journalist Rebecca Tidy mentions in her piece that she occasionally used Encrochat to speak to contacts wishing to maintain anonymity, see https://www.aljazeera.com/features/2021/5/20/the-child-victims-of-the-uks-encrochat-house-raids Abbas Nawrozzadeh also mentions in his piece that "there will be lawyers who have used Encrophones to communicate with their clients", see https://www.aljazeera.com/opinions/2020/7/25/the-encrochat-police-hacking-sets-a-dangerous-precedent. This is confirmed by another article which reports that lawyers in Sweden used EncroChat https://www.svt.se/nyheter/har-lacker-advokaterna-hemlig-information-till-varbynatverket (in Swedish).

categories outside of mandate. The new Europol Regulation confirms the use of predictive policing[42] in European law enforcement as it gives legal footing for the analysis of bulk data by means of "pre-determined criteria" (country of origin, gender, etc.) and self-learning algorithms to single out suspicious persons.[43] However, this kind of data-driven policing suffers from inescapable flaws that pose great risks to the rights and freedoms of individuals: false positives, discriminatory outcomes, opaque processes that are impossible to challenge and a crucial lack of scientific testing or auditing.

Structurally insufficient procedural safeguards: Data-driven investigations, which blur the lines between intelligence and law enforcement practices and purposes, challenge the traditional legal framework of judicial oversight and control.[44] The use by the French Gendarmerie Nationale of "defence secrecy" means that a large part of the information used to justify the launch of criminal investigations remain unknown and impossible to contest. Law enforcement authorities determine by themselves what facts are sufficient to warrant the deployment of intrusive investigative measures such as hacking techniques. The wide margin of appreciation given to the police in defining the nature of the crime and the necessity of interfering measures is in reality barely restricted by an efficient judicial control. This is exemplified in the EncroChat and SkyECC cases by the fact that only a few Encrophones and SkyECC phones found were considered sufficient to confirm the serious criminal nature of the entire communications network and validate its hacking. We observe that the judicial procedure is biased in favour of the investigative interests of the police, in which the investigative judge is pressured to accept all proposed measures. This undermines the adversarial principle, the rights of the defence and the principle of equality of arms.

We therefore consider that bulk hacking must be treated in the same way as bulk interception: its domestic use must be prohibited. State hacking operations must be limited in both time and space. Authorisations for state hacking must include a plan and specific dates to develop and conclude the operation. Furthermore, they should never abuse or target internet and technology service providers, the private sector and critical infrastructures, even in times of conflict.

Instead, they should only target the individual end-user's device or account. State hacking operations must be narrowly designed to return only specific types of authorised information from specific targets and not affect non-targeted users or broad categories of users. Protected information returned outside the clearly-defined limits of the legal authorisation for state hacking in the specific case should be purged immediately.

The use of encryption should not be criminalised and not impede the right to a fair trial

The right to remain silent and the privilege against self-incrimination are key elements of due process rights,

42 Fair Trials, "Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe", 2021 https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf

43 EDRi, "Europol's reform: A future data black hole in European policing", 20 April 2022 https://edri.org/our-work/europols-reform-a-future-data-black-hole-in-european-policing/
Douwe Korff, "The EU's own 'Snowden Scandal': Europol's Data Mining", 19 January 2022 https://edri.org/our-work/the-eus-own-snowden-scandal-europols-data-mining/

44 Maxime Lassalle, L'affaire EncroChat, Recueil Dalloz 2023 p.1833

including the rights of defence and the right to a fair trial under Article 6 of the European Convention on Human Rights (ECHR) and Articles 47 and 48 of the Charter of Fundamental Rights of the European Union.

The use of encryption should not, in any way, affect the full exercise of these rights. We would like to stress that we firmly oppose any form of of coercion in order to get access to encrypted data. This includes laws which require suspects to reveal their password to encrypted systems or devices under the threat of criminal sanctions if they refuse. Such laws are contrary to the prohibition against self-incrimination. We take note of the observation by the HLG that "applying lawful coercive measures to unlock the device in question was reported to be ineffective even in those Member States where the suspect is obliged by law to cooperate."[45] This in itself means that these very intrusive measures are not suitable for the legitimate aim they pursue and cannot be regarded as necessary and proportionate in a democratic society.

However, we would like to highlight a worrying trend in the EU, illustrated notably by the EncroChat and SkyECC cases, where law enforcement and prosecutorial practices target the use of encryption as a sign of criminality and threaten the right to a fair trial.

A notable example of such trend is the French "8 December" case, in which the use of communications encryption tools was equated with signs of clandestinity in order to demonstrate the "terrorist nature" of a group of persons. Tools including mainstream ones like WhatsApp, Signal, Protonmail, Silence, etc. as well as the possession of technical documentation and the organisation of digital training courses were pointed out by the investigative judge as "particularly suspicious". At the initiative of EDRi member La Quadrature du Net, more than 120 signatories denounced in a letter this grossly inappropriate association between encryption and criminal behaviour.[46]

We would welcome if the HLG would take into consideration this dangerous trend, clearly position itself against it and ensure that its final recommendations do not support it.

We remain at the disposal of the HLG working groups for any question related to this submission and for any further comment on other matters of the HLG scope and work.

Appendices

Privacy International, Securing Privacy: PI on End-to-End Encryption, September 2022 (attached) https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf

Privacy International, A technical look at Phone Extraction, 14 October 2019 (attached) https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone

45 Background document for the second plenary, page 4 https://home-affairs.ec.europa.eu/document/download/05963640-de76-4218-82cd-e5d4d88ddf96_en?filename=HLG-background-document-21112023.pdf

46 Tribune Collective, « Attachés aux libertés fondamentales dans l'espace numérique, nous défendons le droit au chiffrement de nos communications », Le Monde (June 2023) https://www.lemonde.fr/idees/article/2023/06/14/attaches-aux-libertes-fondamentales-dans-l-espace-numerique-nous-defendons-le-droit-au-chiffrement-de-nos-communications_6177673_3232.html

%20Extraction%20FINAL.pdf

European Digital Rights, State access to encrypted data, 21 October 2022 (attached) https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf