EDRi

State access to encrypted data

A digital rights perspective

Contributors

Chloé Berthélémy, EDRi
Jesper Lund, IT-Pol Denmark
Bastien Le Querrec, La Quadrature du Net
Rejo Zenger, Bits of Freedom
madonius, Chaos Computer Club
Namrata Maheshwari, Access Now
Gustaf Björksten, Access Now
Rand Hammoud, Access Now
Caterina Rodelli, Access Now
Erica Portnoy, Electronic Frontier Foundation
Andre Meister, individual observer

Index

Executive Summary

Recent developments in EU legislation, policy debates and police operations brought the European Digital Rights (EDRi) network to revisit its position on encryption and the methods deployed by state actors to hack encrypted systems in the context of criminal investigations and state surveillance measures more generally.

Building on the 2017 "Encryption Workarounds: a digital rights perspective" document, this paper once more refutes the misguided notion that encryption is an insurmountable obstacle to investigative authorities. The latest international police operations and the vitality of the spyware market clearly show how encryption can be tampered with.

Given the various degrees of interference with rights and freedoms that some methods of circumvention entail, we draw a distinction between those that are irreconcilable with fundamental rights standards and international legal instruments – and thus must be prohibited – and those that can be warranted in very specific and targeted circumstances.

For the latter, we establish a list of eleven strict conditions that state actors must fulfil if they undertake a hacking operation. We also stress that current law enforcement practices are far from meeting these requirements and continuously infringe upon people's fundamental rights, leading EDRi to call for a presumptive ban on the practice until robust and appropriate safeguards are met.

Lastly, we address the issue of state access to metadata: while it is often given less consideration in debates than encryption, its sensitive nature deserves equal attention and protection. This paper is addressed mainly to European Union institutions and Member States.

1. Introduction

This paper responds to the latest political debates and policy developments on encryption at the European Union (EU) level. The observations it makes and the recommendations it contains are addressed mainly to EU institutions and the governments of its Member States.

This position revises EDRi's 2017 paper, "Encryption Workarounds: a digital rights perspective", and updates it by taking into account the most recent political and operational developments in the field of encryption, notably:

- The 2020 Council of the EU Resolution "Security through encryption and security despite encryption";[1]
- The European Commission's Communication on an EU strategy for a more effective fight against child sexual abuse material (CSAM);[2]
- The Interim Regulation on a temporary derogation from the ePrivacy Directive[3] and the proposal for a permanent Regulation laying down rules to prevent and combat child sexual abuse, along with its accompanying update to the Better Internet for Kids (BiK+) strategy;[4]
- The recent international police operations against encrypted communications networks such as EncroChat[5] and SkyECC,[6] and the Pegasus scandal.[7]

In particular, the recent shift in the EU strategy on encryption towards delegating essential state missions like crime detection and investigation to the private sector calls for a renewed debate with civil society, experts and concerned communities.

We recall that encryption serves the interests of every stakeholder in a democratic society: it protects individuals and communities, supports the economy and secures the government in delivering its missions. [8] As such, it is essential to not undermine the development, availability, integrity and use of encryption in any way.

It is also important that policy decisions, which can so adversely impact the fundamental rights of individuals, are based on evidence and have a solid justification, rather than being guided by what is politically salient – and potentially misleading.

For example, it is worth recalling that the imposition of telecommunications data retention as a law enforcement tool led to the existence of an illegal EU instrument that neither the European Commission nor EU Member States were able to defend credibly in court.[9] Ultimately, it was struck down by the Court of Justice of the European Union (CJEU) as a breach of the Charter of Fundamental Rights of the EU.

It is also worth noting that much of the conversation around encryption is driven by the notion that investigations, and thereby law enforcement, are "going dark"[10] because of encryption.

For example, in June 2021, Europol's Executive Director, Catherine De Bolle, and the district attorney of New York County, Cyrus R. Vance, Jr., described "unregulated encryption" as a "serious investigative challenge in virtually all areas of criminality" and that this, "together with other privacy-enhancing technologies, is allowing for warrant-proof technology which increasingly impedes [...] criminal investigations".[11] Yet, this premise has been repeatedly questioned by many scholars and civil society actors.[12]

One of the many reasons given for why the notion of "going dark" is far overblown, is that even encrypted communications still generate metadata – e.g. who communicated with whom, how often, for how long, how frequently, using what network, etc., which is often more valuable to an investigation than the encrypted content itself.

1 **Council of the European Union, 'Council Resolution on Encryption - Security through encryption and security despite encryption' (24 November 2020)** https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

2 **European Commission, 'EU strategy for a more effective fight against child sexual abuse' (24 September 2020)** https://ec.europa.eu/home-affairs/system/files/2020-07/20200724_com-2020-607-commission-communication_en.pdf

3 **Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse (COM(2020) 568 final)** https://digital-strategy.ec.europa.eu/en/library/interim-regulation-processing-personal-and-other-data-purpose-combatting-child-sexual-abuse

4 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Child-sexual-abuse-online-detection-removal-and-reporting-/public-consultation_en

5 **Ylva Johansson, 'Encrochat shows Europol is irreplaceable in fighting cross border crime' (24 July 2020)** https://ec.europa.eu/commission/commissioners/2019-2024/johansson/blog/encrochat-shows-europol-irreplaceable-fighting-cross-border-crime_en

6 **Europol, 'New major interventions to block encrypted communications of criminal networks' (12 March 2021)** https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

7 **Amnesty International, 'The Pegasus Project: How Amnesty Tech uncovered the spyware scandal – new video' (23 March 2022)** https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/

8 **Read EDRi, Encryption is essential for our democratic freedoms, human rights and the economy in the annex** pag. 38

9 **Melinda Rucz, Sam Kloosterboer, Data Retention Revisited (EDRi, September 2020)** https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

10 **'Going Dark' is a term used "to describe [the] decreasing ability [of law enforcement agencies] to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks". IACP, 'Summit Report. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence' (2015)**

The use of online services for a large number of daily activities, not just interpersonal communications, has substantially increased the amount of metadata potentially available to law enforcement.

Surveillance using metadata can constitute a serious privacy violation,[13] though arguably in ignorance of this, Member State laws are often more permissive on the collection of metadata than on content. Several EDRi members, Privacy International among them,[14] have documented how damaging and overly extensive the use of metadata by law enforcement can be.

The digitisation of nearly every aspect of our society has created an overall increase in the amount of information available to law enforcement. Even though some content is encrypted, it is a small enough portion of an ever-growing data pool that despite the outcries from law enforcement, more information is available for investigative purposes than ever before. This has contributed to the notion that we are in fact in a golden age of surveillance.[15]

The narrative that encrypted systems pose insurmountable barriers to criminal investigations is revealed to be false in practice – a fact acknowledged by the law enforcement community itself.[16]

In cases where accessing encrypted content data is crucial for the investigation, there are still many workarounds available and no system is completely bulletproof.

[11] **Catherine De Bolle, Cyrus R. Vance, Jr., 'The last refuge of the criminal: Encrypted smartphones' Politico (26 July 2021)** https://www.politico.eu/article/the-last-refuge-of-the-criminal-encrypted-smartphones-data-privacy/

[12] **Harvard's Berkman Center for Internet and Society, 'Don't Panic' (1 February 2016)** https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

[13] **The CJEU stated multiple times that retention and access to metadata by public authorities can be as intrusive as content data. Joined cases C-203/15 and C-698/15, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. [2016] para 99.** Big Brother Watch and Others v The United Kingdom Applications nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) para 342.

[14] **Privacy International, 'Report on the National Data Retention Laws since the CJEU's Tele-2/ Watson Judgment' (23 October 2017)** https://www.privacyinternational.org/report/53/report-national-data-retention-laws-cjeus-tele-2watson-judgment

[15] **Peter Swire, 'The Golden Age of Surveillance' Slate (15 July 2015)** https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html

[16] **In June 2022, ISS World Europe hosted a "gathering of Regional Law Enforcement, Intelligence and Homeland Security Analysts, Telecoms as well as Financial Crime Investigators responsible for Cyber Crime Investigation, Electronic Surveillance and Intelligence Gathering" during which one seminar presented methods to "defeat encrypted third party services", claiming as part of its introduction that "You can't defeat today's encryption (at least not that we know of) but law enforcement and the government intelligence community can 'Work around encryption' for a price. Once you identify a target using commercially available encryption products or services (and with enough resources or money) government can defeat the target near 100% of the time."** https://www.issworldtraining.com/iss_europe/index.htm

The crux of this investigative hurdle often lies in the costs and resources it entails. Some methods to circumvent encryption may be financially costly. Yet we believe that this is an indispensable accountability measure and deterrent against abuse and unlawful surveillance operations.

A substantial price tag creates an incentive for investigative authorities to more clearly define the measure's target, the volume of personal data needed, and more generally to carry out investigations with moderation, proportionality and in line with the rule of law.[17]

This paper reviews each state encryption-hacking method – or what we previously called"workaround" – and its singular impact on fundamental rights.

For example, guessing the passphrase/password to access an encryption key is seemingly simple, but social engineering[18] may conflict with the Charter of Fundamental Rights depending on the method used.

For the purpose of this paper, we broadly define "state hacking" as any activity by state actors (e.g. law enforcement agencies, investigative judges or intelligence services) to gain access to information stored on or controlled over a computer system or network without the informed and voluntary consent or action of the user(s) and the service provider – regardless of the purpose.

The issue of state hacking should be examined particularly closely. Recently, we have seen several high-profile examples of states hacking into devices or accounts for law enforcement or national security purposes by exploiting security flaws.

They shed a light on unaccountable, opaque and disproportionate state surveillance powers on the one hand, and on what Edward Snowden coined an "out-of-control Insecurity Industry"[19] on the other. The latter is a prolific, profit-driven market whose sole purpose is the production of vulnerability, and which has resulted in the deaths and detentions of journalists and human rights defenders.[20]

The recent Pegasus scandals[21] sent shock waves across Europe and the world as the spyware was used against prominent politicians, including Spain's Prime Minister, and political opposition in Spain, Poland and Hungary, as well as journalists, human rights defenders and lawyers.[22]

State hacking needs to be considered from the perspective of universal human rights standards, including its interference with the rights to privacy, free expression, and due process. There has yet to be an international public conversation on its scope, impact, and necessary human rights safeguards. The public requires more transparency regarding state hacking – and not just about techniques, targets and volumes, but also how and when hacking activity has had unanticipated impacts, or when it was successful in contributing to criminal justice objectives – in order to measure its proportionality.

In the paper, we identify encryption hacking methods that are unacceptable in a democratic society given their severe and disproportionate interferences with people's fundamental rights and their far-reaching impacts on the integrity and security of encryption systems.

We describe the hacking methods that state actors may use to get access to encrypted data and establish a list of compulsory, cumulative conditions under which these methods can be used. We then highlight the role of metadata in today's criminal investigations, the lack of appropriate safeguards against its mass collection and retention, and recall that metadata is just as sensitive as the actual content of the communications.

Finally, we call for urgent reform of European States' surveillance laws and policies and the regulation of unlawful state hacking practices.

[17] **See, for example,** https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/

[18] **Norton, 'What is social engineering? A definition + techniques to watch for' (26 July 2021)** https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

[19] **Edward Snowden, 'The Insecurity Industry' (26 July 2021)** https://edwardsnowden.substack.com/p/ns-oh-god-how-is-this-legal?

[20] **Forensic Architecture, 'Digital Violence. How the NSO Group enables state terror?'** https://www.digitalviolence.org/

[21] **Forbidden Stories, 'About The Pegasus Project'** https://forbiddenstories.org/about-the-pegasus-project/ **Sam Jones, 'Use of Pegasus spyware on Spain's politicians causing crisis of democracy' The Guardian (15 May 2022)** https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy

[22] **Not that far back, the example of GCHQ's exploitation of Belgacom to place EU institutions under surveillance may still be salient in the reader's mind: Spiegel, 'Britain's GCHQ Hacked Belgian Telecoms Firm' (20 September 2013)** https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

Glossary

Backdoor: an intentionally built-in mechanism used to bypass a system's security measures in order to gain access to that system or its data.

Brute-force attack: consists of an attacker submitting many passwords or passphrases with the hope of eventually finding the correct one in order to access protected data.

Malware: stands for malicious software that is intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorised access to information or systems, deprive users of access to information or, unbeknownst to users, interfere with the user's computer security and privacy.

Metadata: data that provides information about other data. For example, in the case of electronic communications, data that identifies who talks with whom, where and when, rather than the content of the exchange (text messages, images, etc.).

Spyware: a type of malware that aims to gather information about a person or organisation and send it to another entity in a way that harms the user – for example, by violating their privacy or endangering their device's security.

Zero-day vulnerability: describes security vulnerabilities that hackers can use to attack systems. The term "zero-day" refers to the fact that the vendor or developer is not yet aware of the flaw and therefore had “zero day" to fix it.

2. State techniques to circumvent encryption which lead to an unjustified and unacceptable interference with fundamental rights

2.1 Mandated backdoors

A backdoor is a method that bypasses the security measures of a system to gain access to that system or its data. Backdoors are intentionally built-in vulnerabilities, usually mandated by governments to the service provider (that is developing or maintaining the software, computer system, network, or electronic device) to enable access by police or intelligence agencies.

The notion of backdoors is diametrically opposed to the very intent of implementing encryption: a secure digital infrastructure. In other words, mandating backdoors is forcing technology companies to deliberately and substantially weaken the security of their products and betray the confidence of their users. Moreover, backdoors themselves can introduce additional and unintended vulnerabilities to the software.

Without intending to provide an exhaustive list, examples of backdoors include:

2.1.1 Key escrow

The idea of "key escrow" or "key recovery" was widely debated in the 1990s in connection with the US government's Clipper Chip initiative.[23] Key recovery systems provide access to the plaintext of encrypted traffic outside of the normal channel of encryption and decryption. They function by placing decryption keys (or "master keys") in a "vault" managed by a trusted authority or group of trusted authorities, who can break them out when access to the encrypted data is needed.

This technique is especially praised by law enforcement authorities in the case of device encryption.[24] For instance, in the event that the police obtain a phone and need to access its files, they would require

the phone manufacturer (or the designated escrow authority) to retrieve the decryption key from their central key repository.

2.1.2 Ghost proposals

Ghost proposals involve the modification of the encryption system to enable a third-party listener to be silently added to encrypted conversations.

For example, it would allow an investigative officer to be added to a WhatsApp group chat without any warning to its members while remaining invisible to them.

This can only be done with the cooperation of the service provider as it requires the alteration of the key distribution process to secretly distribute illegitimate keys to an external user, as well as modifications to the notification protocols to prevent users from knowing that new, unauthorised third parties have been granted access to their exchanges.[25]

2.1.3 Client-side scanning

Client-side scanning (CSS) methods enable analysis of data in the clear, in real-time and at rest on the user's device.[26]

These systems scan all content (text, images, videos, etc.) on a device or shared in a communication channel. They use content moderation techniques to scan the content against a hash database of selected, known content, or analyse it using machine learning technologies to identify targeted content never seen before.

The end goal is to block and/or report the suspected content to a third party (such as a platform moderator). For example, when someone sends an image corresponding to one that was already identified as illegal and thus included in the matching database, the system will detect it and block its sharing with the intended recipient. It may also be reported to the law enforcement authorities, where this is mandated by law.

If client-side scanning were to be installed on all devices in a population, this would be a blanket measure that is a form of mass surveillance. The way CSS works is identical to "traditional" spyware, except the former is introduced by the software developer and the latter by a third party.

The technical functioning of CSS and spyware and their capacity to observe what the user does on the device are essentially the same.

The 2022 Report of the Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age", warns states against weakening encryption, "including [...] employing systematic screening of people's devices, known as client-side scanning".

The method gained traction after Apple announced in August 2021 it would roll out a new function in iOS that would scan photos backed up to iCloud in order to detect images depicting child sexual abuse.[27] Even though Apple was forced to backtrack its plans after public outcry, the episode has wrongly convinced several

legislators that this practice for monitoring private communications is technically sound and politically desirable.[28]

2.1.4 The fundamental rights impacts of mandated backdoors

The risks posed by any of these types of backdoors are manifold. First, they introduce systemic security vulnerabilities in encrypted systems.

Building a backdoor can be easy, but securing it is impossible. For example, the main inherent issue with any key escrow system is that the server containing the decryption keys represents a universal vulnerability which turns into a target for all manners of attackers.[29]

There is no way a backdoor can be built so that only "the good guys" can use it. Any such vulnerability will be discovered and exploited sooner or later by unintended, and possibly malicious, actors (such as organised criminals, corrupt employees, or hostile foreign intelligence agencies). In 2009, Chinese hackers breached Gmail services using a backdoor originally designed to provide access only to the government of the United States.[30]

By mandating Google to provide them access, the government inadvertently aided malicious actors to access very sensitive information. Backdoors never work as intended. Back in the 1990s, the US government required companies to deliberately "weaken" the strength of encryption keys when exporting technologies to foreign countries.

23 **H. Abelson, R. N. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, and others, 'The risks of key recovery, key escrow, and trusted third-party encryption' (27 May 1997)** http://academiccommons.columbia.edu/catalog/ac:127127

24 **Trevor Timm, 'Your iPhone is now encrypted. The FBI says it'll help kidnappers. Who do you believe?' The Guardian (30 September 2014)** https://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default

25 **For more details, see Internet Society, 'Fact Sheet: Ghost Proposals', (24 March 2020)** https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/

26 **H. Abelson, R. N. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, and C. Troncoso, 'Bugs in our Pockets: The Risks of Client-Side Scanning' (15 October 2021),** https://arxiv.org/abs/2110.07450

27 **EDRi, 'iSpy with my little eye: Apple's u-turn on privacy sets a precedent and threatens everyone's security' (6 August 2021)** https://edri.org/our-work/ispy-with-my-little-eye-apples-u-turn-on-privacy-sets-a-precedent-and-threatens-everyones-security/

28 **EDRi, 'Private and secure communications attacked by European Commission's latest proposal' (11 May 2022)** https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/

29 **Matthew Green, 'How do we build encryption backdoors?' (16 April 2015)** https://blog.cryptographyengineering.com/2015/04/16/how-do-we-build-encryption-backdors/

30 **Bruce Schneier, 'U.S. enables Chinese hacking of Google' (23 January 2010)** https://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html

These export limitations were eventually lifted, but only in 2015 were serious vulnerabilities discovered in the protocol used to secure connections to websites. Due to flaws in the implementation, it was possible to exploit the backdoor decades later.[31] Because backdoors create systemic security risks, the scale of fundamental rights violations is increased tenfold.

Second, and most importantly, backdoors undermine human rights as they undermine encryption at a systemic level.
They impose disproportionate restrictions on the rights to privacy and data protection as they give access to a wide range of intimate information about someone's life. They also restrict the ability of people to fully control their devices and limit what information those devices share.

Because of their severe interferences with privacy rights, backdoors have adverse implications for associated rights such as freedom of opinion and expression, freedom of association and assembly, the right to liberty and security[32] and the right to non-discrimination.

Restricting encryption via mandated backdoors amounts to eroding a means that "is essential if people are to feel secure in freely exchanging information with others on a range of experiences, thoughts and identities, including sensitive health or financial information, knowledge about gender identities and sexual orientation, artistic expression and information in connection with minority status".[33]

It creates a chilling effect as people will not communicate freely owing to the possibility of having their messages or private content checked or accessed upon request by law enforcement or other government agencies and potentially facing consequences.

The risk of self-censorship is global as backdoors affect not only the targeted individuals but everyone using the same means of communication and information. Likewise, security risks are widened to the general population as these techniques create vulnerabilities for anyone, anywhere to exploit. This results in people in hostile environments or unstable political regimes, who rely on encryption to stay safe, being at risk of severe human rights abuses.
For example, for human rights defenders, encryption can be the difference between life and death.[34]

Third, backdoor proposals fundamentally undermine the purpose and trustworthiness of end-to-end encryption. The result is that supposedly confidential communications between the sender and receiver may no longer be confidential, and are less secure. The answer to security problems like those created by terrorism cannot be the creation of further security risks.

Lastly, it is important to realise that mandating backdoors won't stop crime. No matter how far governments' demands go to weaken the security of the products we all use on a day-to-day basis, criminals will either move to non-compliant systems outside the governmental jurisdiction or develop their own encrypted systems.[35]

2.2 Compelled access by forcing self-incrimination or using coercion

Compelling by law and/or forcing the user of a device to give access to the encryption key or the data in clear to law enforcement authorities unacceptably interferes with human rights.

From the perspective of law enforcement, obtaining the key from someone who knows it is comparable to discovering it during a search. However, for the individual concerned, there is a substantial difference between the two situations.

The right to remain silent and the privilege against self-incrimination are key elements of due process rights, 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.[36]

The threat of criminal sanctions if the individual does not disclose a key runs a high risk of unduly interfering with these fundamental rights. A measure allowing authorities to compel the key is likely to be justified by the investigation of very serious offences.

31 **Matthew Green, 'Attack of the week: FREAK (or 'factoring the NSA for fun and profit')', (3 March 2015)** https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/

32 **We recall that the CJEU rejected the interpretation that the right to security under Article 6 of the EU Charter of Fundamental Rights can impose a positive obligation on the State to prevent or punish certain criminal offences. It clarifies in paragraphs 125-127 of La Quadrature du Net and Others that this right protects individuals against arbitrary deprivations of liberty by public authorities.**

33 **United Nations,** https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

34 **Gustaf Björksten, 'Who we hurt when we attack encryption', Access Now (21 October 2021)** https://www.accessnow.org/who-we-hurt-when-we-attack-encryption/

35 **Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner, 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', (6 July 2015)** https://dspace.mit.edu/handle/1721.1/97690

36 **The Court of Justice of the European Union recognised that the Charter provides for a right to remain silent for natural persons in any proceedings potentially leading to sanctions of a criminal nature in its ruling DB v Commissione Nazionale per le Società e la Borsa (Consob) (Case C-481/19). The Court held that the right to silence is infringed upon when a person is forced to testify under threat of criminal sanctions and their testimony is either obtained as a consequence, or they are sanctioned due to their refusal.**

However, in these cases, the measure could be highly ineffective as the alleged perpetrator would prefer criminal sanctions for not disclosing the key over providing law enforcement access to incriminating information which, in the criminal trial facilitated by the disclosure, could lead to a harsher sentence.

This strongly suggests that legal measures to compel the key will mainly be effective for less serious offences where criminal sanctions are comparable to those for not disclosing the key. As such, the measure will be either ineffective or disproportionate.

Forcing access to smartphones is more and more commonly used by law enforcement officers, even in the prosecution of ordinary and petty crimes.[37]

In France, Article 434-15-2 of the Criminal Code – which was declared constitutional in March 2018[38] – punishes people with up to three years imprisonment and a fine of 270 000 euros for the failure to provide "the secret decryption process of a form of cryptology likely to have been used to prepare, facilitate or commit a crime or offence".[39]

This provision was adopted shortly after the 9/11 attacks as part of the law of 15 November 2001, which was intended to combat acts of terrorism and serious crimes. However, it is now used for acts that have little in common with those that justified its creation, highlighting how standards initially intended for exceptional circumstances gradually spill over to ordinary situations.

Moreover, in any system that allows law enforcement to compel the production of a key, there must be allowances in cases where the individual who used the encrypted device may no longer know the password.

A survey conducted by OnePoll in 2021 found that 63% of respondents have been locked out of 10 online accounts per month,[40] while a study by HRPY found that 78% of respondents required a password reset in their personal life within the last 90 days due to forgetting a password.[41] In no situation should a person be detained for failing to provide information that they are unable to provide.

However, it will be very difficult for a court to establish whether an accused individual has really forgotten the password or merely claims so in order to avoid criminal sanctions for not disclosing the key.

The individual cannot prove that they have forgotten the password, and the presumption of innocence must also apply to the crime of not revealing a password known to the individual.

Compelling access to encrypted data or encryption keys is sometimes compared to the obligation to disclose a fingerprint or DNA sample in certain criminal investigations. In these cases, the information disclosed involuntarily by the individual is used for very specific purposes (e.g. comparison with a fingerprint found at a crime scene).

In the context of protection against self-incrimination, this cannot reasonably be compared to being compelled to disclose an encryption key that may give law enforcement access to large amounts of information (e.g. the individual's entire private communications and other data stored on their computer and telephone), which has the potential to reveal large parts of their intimate life, personal history, opinions and beliefs.

Access to private communications also interferes with the privacy and fair trial rights of third persons. In terms of the practical aspects, the analogy with biometric samples is also highly misleading, because a fingerprint or DNA sample can be obtained involuntarily from the individual with moderate physical coercion for a short period.

Subject to appropriate safeguards, this can be a proportionate measure against a suspect in very serious cases (for example, if there is an imminent concrete threat to a person's life or an attempt to the person's dignity and physical safety).

The physical coercion used to disclose the key, however, involves the detention of the individual for a much longer and possibly indeterminate period, which is unlikely to meet the threshold for proportionality for the reasons outlined above.

In cases where keys are held by third parties, other issues arise. For example, a single key may be used to protect the communications of many individuals, making its disclosure inherently disproportionate.

In addition, in any instance where a third party is requested or required to retrieve an encryption key, such surveillance must still comply with user notification principles. Finally, conflict of laws principles must be taken into account where the key that is sought is located in a country other than the one issuing the order.

[37] **AFP, Le Figaro, 'Nancy : six bloqueurs poursuivis en correctionnelle' (6 May 2018)** https://www.lefigaro.fr/flash-actu/2018/05/06/97001-20180506FILWWW00024-nancy-six-bloqueurs-poursuivis-en-correctionnelle.php

[38] **La Quadrature du Net, 'Conseil constitutionnel : La Quadrature plaide contre l'obligation de livrer ses clefs de chiffrement' (6 March 2018)** https://www.laquadrature.net/2018/03/06/conseil-constitutionnel-clefs-chiffrement/

[39] **The Constitutional Council refused the interpretation that a phone access code (e.g. PIN or unlock code) is excluded from the scope of this article because it is not an encryption key. La Quadrature du Net warned that "this decision calls into question the right to encryption and the value of its use, but also, incidentally, privacy, the confidentiality of communications, the confidentiality of journalistic sources and freedom of communication". See: La Quadrature Net, 'Le Conseil constitutionnel restreint le droit au chiffrement' (4 April 2018)** https://www.laquadrature.net/2018/04/04/le-conseil-constitutionnel-restreint-le-droit-au-chiffrement/

[40] **OnePoll, 'Password anxiety' (2021)** https://www.onepoll.us/portfolio/lastpass-password-anxiety/

[41] **HYPR, 'Study Finds 78% of People Reset a Password They Forgot in Past 90 Days' (10 December 2019)** https://blog.hypr.com/hypr-password-study-findings

3. Regulating state hacking

3.1 State techniques to circumvent encryption without compelled assistance from the individual or service provider

The following section attempts to describe and categorise the various techniques employed by state actors to get access to encrypted data without any intervention from targeted users or service providers.

They do so either by using circumventing methods that do not exploit technical flaws in the system (e.g. obtaining the decryption key), or by actively researching and exploiting technical flaws in the security system.

Given the severe degree of interference with human rights that state hacking entails, in this section we also establish a list of eleven conditions that state actors must fulfil before engaging in such practices, for their operations to be considered proportionate and acceptable in a democratic society.

Unlike the two workarounds previously described (see "Mandated Backdoors" and "Compelled access by forcing self-incrimination or using coercion" above), which by design can never be limited, justified or acceptable, the following techniques can potentially be used in ways that are acceptable in a democratic society.

However, state hacking needs to be strictly regulated. The necessary safeguards are discussed in a separate section below.

3.1.1 Circumvention methods that do not exploit technical flaws in the system

If investigative authorities can gain access to the (unprotected) key or the password for a system, they can access the encrypted content in the same way as the intended user.

The common denominator of these methods is that they do not interfere with the technical workings of the encryption system. We include them under "state hacking" because the access to the system is "unauthorised" from the viewpoint of the user, and because the legal safeguards discussed below should apply to these methods as well.

There are several circumstances under which authorities may gain access to a key or password. Choosing and remembering good passwords is notoriously hard, and some people use passwords that are easily guessable, for example because the password is derived from their favourite football team, the name of their partner or children, or other publicly-available information.

This may allow investigative authorities to guess the password within the number of attempts permitted by the system under its normal operation. Some methods for guessing passwords involve modifying the technical workings of the system so that more attempts are allowed. They are included in the next sub-section.

The password could be written on a piece of paper which is hidden in a "secret" place discovered by investigative authorities during a physical search of the suspect's premises. Video surveillance of the suspect could also be used to obtain knowledge of the password. Another method is gaining access to a digital file where the password is stored, such as an unlocked password manager, or accessing the plaintext (unencrypted content) directly when in use by the suspect on a computer or smartphone. This strategy may involve an element of deception to trick the suspect into leaving the device unattended for a short time. The mastermind of the darknet market website Silk Road was apprehended in this way.[42]

Other forms of social engineering or deception could be used to get access to either the key/password or a copy of the plaintext. Deception is a long-standing law enforcement practice, but the laws of Member States typically restrict some forms of it. For example, German courts have developed special rules where affirmative misrepresentation is barred, and misimpressions about the law must also be corrected. Questioning by undercover agents in jail is prohibited, on the grounds that it violates the rules of detention.[43]

3.1.2 Exploiting technical flaws in the system

Most systems impose limits on the number of wrong passwords that can be entered, either as a hard limit (after which the system shuts down permanently and auto-erases the content) or by progressively increasing the delay between consecutive attempts when incorrect passwords are entered.

[42] **Natasha Bertrand, 'The FBI staged a lovers' fight to catch the kingpin of the web's biggest illegal drug marketplace' Business Insider (29 May 2015)** https://www.businessinsider.com/ross-ulbricht-will-be-sentenced-soon--heres-how-he-was-arrested-2015-5

[43] **Christopher Slobogin, 'An Empirically Based Comparison of American and European Regulatory Approaches to Police Investigation', 22 M ICH . J. I NT ' L L. 423 (2001)** https://repository.law.umich.edu/mjil/vol22/iss3/3

Investigative authorities could try to bypass these limitations, either by exploiting existing flaws in the system (software) or by compelling the system's vendor to remove the protection against brute-force attacks.

The investigation of the 2015 San Bernardino attack in the US provides a widely publicised account of both approaches. First, the FBI tried to obtain a court order compelling Apple to modify the operating system on the (deceased) perpetrator's iPhone, so that brute-forcing could be used to unlock the device. Apple opposed this order on grounds that it was an unprecedented step which threatened the security of all Apple customers.

The case was never decided by US courts because the FBI withdrew the request in March 2016 after a third party was able to assist them in unlocking the device by exploiting an unknown software flaw (zero-day vulnerability) on the particular iPhone model used by the perpetrator. [44]

Compared to the above-mentioned approaches of discovering passwords from a piece of paper or through video surveillance of the suspect, methods which exploit technical flaws are much more problematic.

The zero-day vulnerability that allowed the FBI to unlock the iPhone in the San Bernardino case could also be used by malicious actors, and such software vulnerabilities must be reported to the vendor and fixed as soon as possible. When investigative methods rely on the availability of unpatched vulnerabilities, there is at the very least a conflict of interest for the state.[45]

Even more concerning are laws requiring the vendor to deliberately introduce software flaws by removing security functionality, similar to what the FBI sought in the San Bernardino case by invoking an ancient law from 1789 (All Writs Act). This is tantamount to undermining encryption outright,[46] and is therefore unacceptable as outlined in the "Mandated Backdoors"section above.

The Israeli company Cellebrite offers a product series, UFED (Universal Forensics Extraction Device), which can extract data even from locked smartphones in certain cases.[47] UFED is widely used by law enforcement authorities throughout the world.

Information extraction by brute-force methods, and indeed the use of Cellebrite UFED, generally requires physical access to the person's device. This is not the case for methods that install spyware (malware) on the user's device to capture passwords with keyloggers, exfiltrate plaintext copies of encrypted documents, or access private communications before transmission where the content is end-to-end encrypted.

Although the user can sometimes be tricked into installing spyware apps on a computer or smartphone, the spyware infection ("installation") commonly relies on zero-day vulnerabilities at the operating system level. The most potent attack vectors are the so-called "zero-click"

vulnerabilities where the user's device can be infected simply by receiving a malicious text message without any user interaction through deception (such as clicking on an "interesting" link in a text message).

The Pegasus spyware from the Israeli company NSO is known to rely on zero-click vulnerabilities. NSO is part of the highly controversial spyware industry that offers malicious software infections as a service to government actors in states that abide by the rule of law, but also in states that don't. Once installed, the spyware can potentially extract (exfiltrate) any information on the user's device or any cloud storage accessible from the user's device.

The spying capabilities do not stop with data extraction. By secretly activating the microphone or camera, the spyware can turn the user's smartphone or computer into an eavesdropping or video surveillance device. It can also keylog[48] and capture user input in real-time, including passwords and data from other third-party services.

Needless to say, all of these methods are highly intrusive and many of them do not pass the test of our eleven fundamental conditions to strictly regulate state hacking (listed in the section below). If such standards cannot be reached – by design or in practice – then such methods and tools will not be permissible in a democratic, rule-of-law society.

[44] **Originally, the Israeli company Cellebrite was believed to have secretly assisted the FBI. In April 2021, it was revealed by the Washington Post that a small Australian white hat hacking firm had helped the FBI. Ellen Nakashima, Reed Albergotti, 'The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm' The Washington Post (14 April 2021)** https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/

[45] **In Council Document 7675/20 LIMITE, the EU Counter-Terrorism Coordinator complains that "service providers are unilaterally implementing changes to their encryption practices, without actually engaging with the EU or Member States to address concerns of law enforcement and judicial authorities in the roll-out", citing an example with security upgrades on Android smartphones (described in the article 'Head of Android Security Says Locking Out Law Enforcement Is an 'Unintended Side Effect", VICE (30 January 2019)** https://www.vice.com/en/article/yw8vm7/android-security-locking-out-law-enforcement-unintended-side-effect **Leaked version of the LIMITE Council document is available at:** https://www.statewatch.org/media/1435/eu-council-encryption-ctc-paper-7675-20.pdf

[46] **Access Now, 'Brief Of Amici Curiae Access Now And Wickr Foundation In Support Of Apple Inc .'S Motion To Vacate' (22 March 2016)** https://www.accessnow.org/cms/assets/uploads/2016/03/Apple-Amicus-Brief-Access-Now-Wickr-Fndtn.pdf

[47] **It is unclear to what extent Cellebrite UFED relies on software vulnerabilities for unlocking smartphones, and whether UFED is able to bypass the security of the most modern smartphones. The widely advertised capabilities of Cellebrite UFED are disputed by Moxie Marlinspike in the blog post 'Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective' (21 April 2021)** https://signal.org/blog/cellebrite-vulnerabilities/ **However, Privacy International reported that a technical expert working for Cellebrite had confirmed to them that "[they] have exploits". See Privacy International, 'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers' (3 April 2019)** https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

[48] **Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored.**

3.2 Eleven fundamental conditions for state hacking

We call for a presumptive ban on state hacking until all the following safeguards are met. These conditions are cumulative. If one is not met, the hacking must be considered unlawful, and thus prohibited.

3.2.1 Meet the "quality of law" requirements

State hacking must be provided for by laws that are clearly written, accessible, publicly available and in line with the principle of foreseeability[49], and that specify the narrow circumstances in which it could be authorised. State hacking must never occur with either a discriminatory purpose or effect.[50]

3.2.2 Demonstrate strict necessity and proportionality

State actors must be able to clearly explain why hacking is the least invasive means of getting protected information in every case where it is to be authorised, as well as why it is adequate and relevant. In each of these cases, they must also connect that necessity back to one of the statutory purposes provided.

The strict necessity should be demonstrated for every type of protected information that is sought, which must be identified ex-ante, and for every user (and device) that is targeted. Safeguards should be put in place with regard to the right to access specific information on a decrypted device, not least due to the extensive and, by default, highly sensitive data that can be stored on or accessed by a device.

In addition, to respect the principle of proportionality, state hacking operations should be restricted to the prosecution of very serious types of crime. Given the gravity of the interference with fundamental rights such access entails, it has to be proportionate to the legitimate aim pursued. Thus, only the objective of combating serious crime is capable of justifying it, in line with the CJEU's jurisprudence on data retention.[51]

However, we also note that the definition of serious crimes has greatly fluctuated and worryingly inflated over the past years.

The attempt to circumscribe serious crimes in EU law often takes as a basis the gravity of the sanction (e.g. maximum custodial sentence of at least X number of years) but, in practice, this threshold tends to encompass a broad range of offences, including petty crimes, which puts into question its validity and legitimacy to define serious crimes.[52]

Lastly, hacking operations are not proportionate when they violate professional secrecy and legal professional privilege by accessing protected material and confidential communications between lawyers and their clients, doctors and their patients, journalists and their sources, or religious counsellors and their beneficiaries.

Professional secrecy is a vitally important principle that, in a democratic country, guarantees fundamental rights such as the rights of the defence, the right to health care, freedom of expression and information, freedom of thought and religion, etc.

Pegasus spyware

Pegasus is hacking software that is developed, marketed and licensed to governments by the Israeli company NSO Group. Amnesty International and Forbidden Stories revealed in July 2021 that the software "has been used to facilitate human rights violations around the world on a massive scale, following the revelation of 50 000 phone numbers of potential surveillance targets."

Their research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated against journalists, political opponents and human rights defenders.

Exploiting "zero-day" vulnerabilities, Pegasus can read, send and receive messages (even those that are end-to-end encrypted), download stored photos, access and control various phone functionalities like the microphone and camera, and access the geolocation module. It grants complete, unrestricted access to the device and thus to the entire personal data it contains.

In his "Preliminary Remarks on Modern Spyware", the European Data Protection Supervisor (EDPS) argues that the level of interference with the right to privacy is "so severe that the individual is in fact deprived of it".[54]

[49] Individuals should be able to foresee to a reasonable extent what repercussions certain actions or inactions will have under the law.

[50] Data must be collected and analysed to assess any such effects, against which action can then be taken.

[51] Joined Cases 511/18, C-512/18 and 520/18 La Quadrature du Net and Others v Premier ministre and Others [2020]

[52] For instance, in the European Commission's e-evidence legislative proposals, the issuance of a production or preservation order to obtain access to or ask for the retention of data held by private service providers is conditional to the investigation and prosecution of crimes punishable by a maximum of at least three years imprisonment. EDRi has argued that the definition also covers smaller offences such as simple theft, fraud or assault under the criminal codes of some Member States, which is not proportionate considering the serious interference with fundamental rights this instrument may entail. See EDRi, 'Recommendations on cross-border access to data: Position paper on the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters' (25 April 2019) https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf

[53] Amnesty International, 'Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally' (19 July 2021) https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[54] European Data Protection Supervisor (EDPS), 'Preliminary Remarks on Modern Spyware' (15 February 2022) https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

He concludes that Pegasus and similar highly-intrusive spyware technology can affect the essence of our fundamental rights. Indeed, accessing such large, unrestricted and undefined amounts of highly sensitive data in real-time cannot possibly be reasonable and cannot pass the test of proportionality.

Beyond the intrusive nature of the tool itself, the Pegasus revelations have proven that many safeguards listed in this paper are not respected by states and that abuses were systemic. The software was in large part used to pursue politically motivated goals such as the unlawful surveillance and repression of civil society actors, members of the press and political dissidents. The use, sale and transfer of such surveillance technology should therefore be prohibited as soon as possible.

Mainstreaming of invasive hacking techniques against ordinary crimes and for the surveillance of marginalised groups

Access and use of hacking techniques are being mainstreamed for an increasing range of law enforcement actors (including immigration control authorities).

As a result, very privacy-intrusive methods are being used in day-to-day police work, notably to investigate petty crimes, and for other policy objectives which do not justify such severe encroachment on people's fundamental rights – such as preventing unauthorised asylum grants or deporting rejected asylum seekers more quickly.

This is partly explained by the fact that acquiring and using hacking tools has become much easier, notably phone extraction technology. VICE already reported in 2016 that Cellebrite's[55] products were no longer solely used by US federal agencies but also by local bodies for the prosecution of "any and all crimes".

In 2019, the French national police announced at Milipol, the world exhibition dedicated to internal security, that it would deploy 500 of Cellebrite's phone cracking and forensic UFEDs in local police stations across the territory by 2024.[57] Surveillance technology companies provide products that are more "user-friendly", require little to no training and are portable (laptop-sized or handheld devices), which enables their wider deployment.

While the sale of such technologies to authoritarian regimes, where they are used to repress human rights activists, was already established,[58] reports also point to the use of phone extraction methods to investigate the digital lives of people on the move and seeking asylum.[59]

As reported by EDRi member Privacy International, Cellebrite's Vice President of International Marketing pointed out in Morocco to government officials that their technology could be useful to extract information from phones of people without documents, to find out who they are, what they have been doing, where they have been, when, and ultimately why they are seeking asylum.

EDRi member Gesellschaft für Freiheitsrechte also demonstrated how the German Federal Office for Migration and Refugees has routinely been reading and analysing data from electronic devices in order to determine their owner's origin and identity, in conflict with various data protection rules.[60]

Such cases show how the expansion of these technologies for other purposes and to other parts of the population beyond the fight against serious crimes is a very concrete, current threat.

Regardless of whether or not the tools exploit vulnerabilities in devices' software, the technique leads to the wide collection of sensitive data,[61] including data that is not necessarily relevant to the investigation or the administrative procedure. This constitutes a disproportionate interference with the right to privacy prohibited by the Law Enforcement Directive.[62]

Moreover, it severely undermines the right to asylum and a fair procedure in the case of phone data extraction during the evaluation of asylum applications. However, it is likely that, in practice, the mass extraction of data is not supervised and prevented.[63]

55 **See sub-section 'Exploiting technical flaws in the system', pages 13 and 14 of this paper for a description of the firm Cellebrite and its flagship product.**

56 **Joseph Cox, 'US State Police Have Spent Millions on Israeli Phone Cracking Tech' VICE (21 December 2016)** https://www.vice.com/en/article/aekqkj/us-state-police-have-spent-millions-on-israeli-phone-cracking-tech-cellebrite

57 **Émilie Massemin and Isabelle Rimbert, 'Nous avons visité Milipol, le salon de la répression' Reporterre (25 November 2019)** https://reporterre.net/Nous-avons-visite-Milipol-le-salon-de-la-repression

58 **Joseph Cox, 'Cellebrite Sold Phone Hacking Tech to Repressive Regimes, Data Suggests' VICE (12 January 2017)** https://www.vice.com/en/article/aekqjj/cellebrite-sold-phone-hacking-tech-to-repressive-regimes-data-suggests **Oded Yaron, 'Human Rights Activists Urge Israel to Stop Spy Tool Exports to Hong Kong Police' Haaretz (28 July 2020)** https://www.haaretz.com/israel-news/2020-07-28/ty-article/.premium/human-rights-activists-urge-israel-to-stop-spy-tool-exports-to-hong-kong-police/0000017f-e35a-d804-ad7f-f3fae4b80000

59 **Privacy International, 'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers' (3 April 2019)** https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

60 **Gesellschaft für Freiheitsrechte e.V., 'Invading Refugees' Phones: Digital Forms of Migration Control in Germany and Europe' (February 2020)** https://legacy.freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf

61 **Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual orientation, etc.**

62 **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89**

63 **A police officer conceded to a journalist that "Even if the software allows it [make a targeted data collection], it doesn't mean that colleagues on the ground will necessarily use it that way, the easiest thing is to extract everything and then sort it out." See Christophe-Cécil Garnier, 'Bientôt dans presque tous les commissariats, un logiciel pour fouiller dans vos portables' StreetPress (20 January 2020)** https://www.streetpress.com/sujet/1579520319-police-gendarmerie-un-logiciel-pour-fouiller-portables

3.2.3 Prohibit unrestricted and bulk hacking

Bulk hacking must be treated in the same way as bulk intercept; 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.

From that perspective, bulk hacking must be prohibited, including not just the hacking of large numbers of devices, but also the use of hacking techniques to collect information on large numbers of people from centralised systems.

To illustrate the importance of this safeguard, it is worth remembering that Snowden revealed that GCHQ was harvesting Gmail and other Google data in bulk from the backup data flows between Google data centres in different countries and notably to place EU institutions under surveillance.[64]

Encrochat and SkyECC bulk hacking operations

EncroChat was an encrypted phone network used by some criminal networks.[65] In a joint investigation operation, law enforcement authorities in France and the Netherlands obtained access to electronic communications data for a large number of individuals suspected of various crimes.

Communications data from the EncroChat network was obtained in a general and indiscriminate manner where all users were subjected to bulk hacking (sometimes referred to as "bulk equipment interference"). The data was subsequently shared with many other states through Europol, the EU's police cooperation agency.

Instead of an individualised suspicion to justify the extremely intrusive measure of government hacking and interception of private communications, the French and Dutch authorities simply assumed that most EncroChat users were criminals.[66]

Clearly, the French and Dutch authorities could not reasonably have known this beforehand due to the highly anonymous nature of the EncroChat network (which in itself is not illegal).

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 the law granting special protection to data and communications exchanged between lawyers and their

clients[67] or between journalists and their sources. The EncroChat user-base is also likely to have included journalists, whistleblowers and human rights defenders,[68] all of whom have legitimate needs for strong privacy protection. 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.

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.

Furthermore, since the users of EncroChat 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.

When Europol analyses and "distributes" communications data obtained in bulk in this manner, at least some Member States' authorities may receive information that they could never have obtained legally in a domestic investigation. This raises several issues related to the right to a fair trial, especially as the origin of the information received via Europol may not be fully revealed in the domestic investigation.

64 **Spiegel, 'Britain's GCHQ Hacked Belgian Telecoms Firm' (20 September 2013)** https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

65 **Joseph Cox, 'How Police Secretly Took Over a Global Phone Network for Organized Crime' VICE (2 July 2020)** https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked

66 **The French authorities claimed that they estimated that no less than 90% of EncroChat clients were linked to organised crime. If these numbers are true, it means that potentially up to 6000 users had their fundamental right to privacy infringed. See France24, 'European police shut criminal phone network used to plan murders'(2 July 2020)** https://www.france24.com/en/20200702-european-police-shut-criminal-phone-network-used-to-plan-murders

67 **CCBE, 'Position Paper on the Proposal for Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' (6 May 2021)** https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20210506_CCBE-position-paper-on-Europol-s-mandate.pdf

68 **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).**

3.2.4 Secure independent judicial authorisation

Applications for government hacking must be sufficiently detailed and approved by a competent judicial authority that is legally and practically independent from the entity requesting the authorisation.

This judicial authority should also have access to sufficient technical expertise to understand the full nature of the application and any likely collateral damage that may result. State hacking should never occur prior to judicial authorisation.

Why hacking by intelligence agencies is unacceptable

At the request of the European Parliament, the Fundamental Rights Agency (FRA) produced a study in 2017 on intelligence services in the EU.[69] FRA's research findings show the limits to full independence that several national oversight bodies suffer from.

The main problems identified are that some bodies remain strongly dependent on the executive, do not have binding decision-making powers, have limited staff and budget (or their offices are located in government buildings), have insufficient technical capacity, or are left out when it comes to international intelligence operations.

In light of the above requirement for independent judicial supervision and authorisation, as well as the deficiencies of current oversight systems in Europe, intelligence agencies should not be allowed to carry out hacking operations.

3.2.5 Notify all individuals affected

State hacking must always provide actual notice to the target of the operation and, when practicable, also to all owners of devices or networks directly impacted by the tool or technique once the investigation phase is finished or otherwise once the national legislation allows the disclosure of this information in analogous situations, such as wiretapping.[70]

3.2.6 Increase transparency

Agencies conducting state hacking should publish at least annual reports that indicate the extent of state hacking operations, including at a minimum the authority responsible for carrying the operations and those authorising them, the users impacted, the devices impacted, the length of the operations, and any unexpected consequences of the operation. They should also provide credible, peer-reviewable information on the level of "false positives" (innocent people being wrongly surveilled) and the discriminatory impacts of their activities.

3.2.7 Do not force private providers to weaken their own products

State hacking operations must never compel private entities to engage in activity that impacts their own products and services in a way that undermines digital security.

The San Bernardino case: how the FBI tried to compel Apple to weaken their own products' security

In 2016, the Federal Bureau of Investigation (FBI) ordered Apple to assist in unlocking an iPhone 5C that it recovered from one of

the perpetrators of the 2015 terrorist attack in San Bernardino, California.

The work phone was locked with a four-digit password and was set to eliminate all its data after ten failed password attempts (a common anti-theft measure on smartphones).[71] Apple refused to create a backdoor in its security system which would have disabled the auto-erase function, stating at the time that "The government suggests this tool could only be used once, on one phone.

But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. [...] The government is asking Apple to hack [their] own users and undermine decades of security advancements that protect [their] customers [...] from sophisticated hackers and cybercriminals."[72]

The FBI eventually withdrew its court order application as they found a company able to exploit a zero-day vulnerability in the iPhone's software and bypass the ten-try limitation.[73]

As explained in "Mandated Backdoors" above, this circumvention technique is very perilous as it undermines the entire system, and thereby the security of all users. It also increases the risk of the backdoor getting into unauthorised hands, with the severe damage this can lead to.

Lastly, it creates a dangerous legal precedent, encouraging further government requests for additional backdoors in an ever-growing number of cases.[74]

3.2.8 Stay within the limits of the authorisation

A state operation must never exceed the scope of its authorisation. All data collected or accessed outside of the mandate granted by the independent judicial authority should be immediately deleted, affected individuals notified of the infringement of their rights and of available legal remedies, and the unlawfully collected data should be declared inadmissible as evidence in courts of law.

3.2.9 Respect the principles of international judicial cooperation

Extraterritorial government hacking should not occur absent authorisation from a competent independent judicial authority in the targeted country under principles of dual criminality and without respecting other principles of international law.

3.2.10 Do not stockpile vulnerabilities

State agencies conducting hacking must not stockpile vulnerabilities and, instead, should inform the providers of encrypted systems as soon as possible of any vulnerabilities discovered.

Stockpiling vulnerabilities is very dangerous for the security of systems and devices as it increases the risk of others, including malicious actors, discovering and exploiting those vulnerabilities.

The longer vulnerabilities are stockpiled, the greater the chance they will be discovered and exploited by other parties before they can be fixed by the software vendor. State authorities should not purchase or keep open any vulnerabilities.

In particular, they must never use zero-day vulnerabilities and instead always work to close them as quickly as possible. They should release reports at least annually on the discovery of vulnerabilities.

3.2.11 Do not outsource the search and exploitation of vulnerabilities

In a democratic society, state actors – subject to transparency and accountability measures and human rights safeguards – that engage in any form of hacking must rely on their own internal capacities and resources to carry out their operations while maintaining responsible disclosure when discovering vulnerabilities.

In particular, the search for vulnerabilities in software, devices, etc., as well as their exploitation and the execution of a hack, must not be outsourced to the private sector, domestic or foreign.[75]

[69] **Fundamental Rights Agency, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update' (2017)** https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

[70] **This right to be informed ex post facto must not be undermined by deleting the person's personal data in order to avoid complying with a data subject's access request. See Chloé Berthélémy, 'Rather delete than comply: how Europol snubbed data subject rights' EDRi (28 September 2022)** https://edri.org/our-work/rather-delete-than-comply-how-europol-snubbed-data-subject-rights/

[71] https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute

[72] **Tim Cook, 'A Message to Our Customers' Apple Inc. (16 February 2016). Retrieved from** https://web.archive.org/web/20160217084120/http://www.apple.com/customer-letter/

otnote 31

[74] **Electronic Frontier Foundation, 'The FBI Could Have Gotten Into the San Bernardino Shooter's iPhone, But Leadership Didn't Say That' (2 April 2018)** https://www.eff.org/fr/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say

[75] **We are not supporting the idea that research of vulnerabilities in software, such as penetration testing, should be an exclusive government function. So-called "white hat hacking" is key to the security of systems and devices. Research to find flaws in systems for the purpose of fixing them should be encouraged and remain independent from state control.**

4. The role of metadata in today's criminal investigations

Encryption protects the content of electronic communications or other information, not the associated metadata.

The amount of metadata that is stored by the service provider or that can be intercepted in real-time by law enforcement depends on the technical set-up of the specific electronic communications service.

Therefore, it varies from service provider to service provider, even when the same encryption technology is used.

According to a document from the FBI obtained via a freedom of information (FOI) request, US law enforcement can get real-time access to information about the sender and recipient of WhatsApp messages with a "pen register" order (approved by a judge), whereas the Signal service is designed in such a way that this information cannot readily be extracted for disclosure to third parties.[76]

In addition to the metadata processed by the electronic communications service provider itself, when using the service, internet traffic also generates metadata to transmit the (encrypted) Internet Protocol (IP) packets.

Metadata about usage patterns and location is also generated and stored on communication devices such as smartphones. Although device encryption may prevent direct access to this metadata by adversaries (if properly secured with good passwords), many users rely on cloud services (in particular, US cloud services) for backup, e.g. iCloud, where US law enforcement can obtain access to the data in unencrypted form.

The generation and storage of metadata by online services are largely outside the control of service users.

The information provided to users tends to focus on end-to-end encryption of content, not processing and storage of metadata.[77]

Privacy policies are often rather vague or misleading regarding the storage of metadata. This practical reality even applies to services that claim to offer increased privacy protections by obscuring metadata patterns.

Virtual Private Network (VPN) services offer to hide the IP address of the user, but at the same time, the VPN service provider can collect a lot of metadata about internet usage patterns. By connecting the dots of metadata across different services, law enforcement may be able to identify the user being investigated.[78]

While law enforcement may face obstacles to accessing communications content when end-to-end encryption is used, they still benefit from a golden age of surveillance for metadata.

There are no indications that this will change in the foreseeable future, but rather the contrary, as the use of online services and smart home devices connected to the cloud continues to increase.

While it is sometimes possible to obfuscate the metadata trail with certain anonymisation services, the use of such services comes with the inherent risk that even more metadata will be generated.

Some intelligence services are known to operate bulk interception schemes for internet traffic by tapping fibre-optic cables or switches at internet exchanges.

Even if the content of the internet traffic is effectively protected with encryption, e.g. state-of-the-art TLS (transport layer security) with forward secrecy, the associated metadata of the internet packets will still be intercepted.[79]

The Snowden documents revealed that GCHQ secretly monitored visitors to a Wikileaks site by collecting their IP addresses. These IP addresses can then be used as selectors for further collection and analysis of internet traffic, e.g. for building dossiers of the most frequent visitors to Wikileaks, a group of persons that is likely to include journalists, whistleblowers and human rights activists.

The Tor network and VPN services that seek to anonymise the source and destination of internet traffic can also be monitored and possibly de-anonymised through correlation analysis of metadata from internet packets entering and leaving these networks.

Surveillance of metadata constitutes a serious interference with the right to privacy and other fundamental rights. Civil society organisations have long argued and documented that metadata can be as revealing about the private life of individuals as the content of their communications.

This is especially true because metadata lends itself much more readily to a systematic analysis by automated means and the creation of profiles for the individuals concerned.[80]

Recent rulings from the CJEU and the European Court of Human Rights have recognised that bulk collection and retention of metadata is just as sensitive as the actual content of the communications.[81]

Therefore, metadata should be given the same legal protection as the content of communications, in particular when metadata is systematically collected.

However, in reality, metadata is often not afforded the same legal protection as content in the national law of EU Member States.

76 Catalin Cimpanu, 'FBI document shows what data can be obtained from encrypted messaging apps' The Record (30 November 2021) https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/

77 Norwegian Consumer Council, '250,000 words of app terms and conditions' (24 May 2016) https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/

78 Richard Chirgwin, 'VPN logs helped unmask alleged 'net stalker, say feds' The Register (8 October 2017) https://www.theregister.com/2017/10/08/vpn_logs_helped_unmask_alleged_net_stalker_say_feds/

79 If forward secrecy is not employed, e.g. because it is not supported by both endpoints of the communication or because of an active TLS downgrade attack against the communication, encrypted internet packets can be stored and possibly decrypted at a later date if the encryption keys from the online server are somehow compromised.

80 Privacy International, 'Report on the National Data Retention Laws since the CJEU's Tele-2/ Watson Judgment' (23 October 2017) https://www.privacyinternational.org/report/53/report-national-data-retention-laws-cjeus-tele-2watson-judgment

81 Joined cases C-203/15 and C-698/15, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. [2016] para 99. Big Brother Watch and Others v The United Kingdom Applications nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) para 342.

5. Conclusion

This paper demonstrates that the myth that encryption harms policing is not substantiated: "The world did not 'go dark'.

On the contrary, law enforcement has much better and more effective surveillance capabilities now than it did then."[82] Crucially, however, many methods to access encrypted data (like the Pegasus spyware, key escrows or client-side scanning), even when deployed in purportedly limited ways, cannot meet fundamental rights standards and must be explicitly rejected.

Likewise, the practice of forcing someone to self-incriminate by providing their decryption key is too severe an encroachment on fundamental fair trial rights, and thus constitutes a red line in a democratic society.

Nonetheless, there are lawful and legitimate methods of investigating serious crimes even when evidence is potentially held in encrypted data.

For these other techniques, in this paper we have developed a set of eleven conditions to strictly define the circumstances under which they may be used by state actors without unduly infringing on rights and freedoms. If one of these conditions is not met, the hacking must be considered unlawful.

They aim to guarantee that state hacking is limited in both time and space, is targeted, accountable and proportionate, respects individuals' fundamental rights, is controlled by independent oversight, and that its negative impacts on the integrity and security of encrypted systems are limited as much as possible.

Taking into account the extensive case law of the European Court of Human Rights and the EU Court of Justice, we believe that if state hacking takes place in circumstances that do not meet our eleven conditions, it will be in breach of both the European Convention on Human Rights and the EU Charter of Fundamental Rights.

Yet many law enforcement agencies are actively using unchecked hacking tools, benefiting from loopholes or the absence of national legislation on the issue.

All recent examples, the Pegasus scandal first and foremost, show the complete absence of safeguards against invasive surveillance measures.

These practices directly infringe upon individuals' rights under international legal instruments, including the Charter of Fundamental Rights. Therefore, while EDRi recognises human rights-compliant state hacking as theoretically possible in very strictly controlled and limited cases, we call for a presumptive ban on the practice until robust and appropriate safeguards are met.

Lastly, we also discussed the use of metadata in the context of criminal investigations, since it is often depicted as a good alternative to obtaining information when content data is inaccessible, but is also not considered a type of sensitive data collection.

However, as stated in successive rulings by the highest courts of justice in Europe, metadata may reveal very intimate details about someone's life and is thus of a sensitive nature. It is therefore crucial to regulate access to metadata by law enforcement authorities with the same level of protection as content data to respect people's right to privacy and data protection.

We are committed to helping European institutions and governments to the best of our ability and capacity in achieving a rights-respecting framework for law enforcement access to personal data.

82 **Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner, 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', (6 July 2015)** https://dspace.mit.edu/handle/1721.1/97690

Encryption is essential for our democratic freedoms, human rights and the economy

Annex

The availability and use of encryption is essential for the protection of our digital infrastructure and communications. It is not only important for our democratic freedoms, but also vital for innovation and economic growth.

Therefore, all governments must:

- support the development of encryption;
- encourage the use of encryption in an
- openly accessible manner for everybody;
- and not in any way undermine the development, availability and use of encryption.[i]

Encryption is the technology which secures information by making it incomprehensible to anyone other than the entities authorised to access it by the application of a mathematical process.[ii]

Encryption can protect data in transit, when it travels across the internet and at rest, when it is stored in a server or on a smartphone for example.

One particular form of encryption is end-to-end encryption, which ensures that only the sender and the intended recipient can read the encrypted information.

If this principle is compromised in any way or if any of the components of encryption (the original text, the encryption algorithm and the keys to encrypt and decrypt) are attacked, the effectiveness and integrity of encryption are no longer guaranteed.[iii]

Everyone relies on Encryption

The protection of digital communication is essential for people's autonomy in any modern society. Encryption enables us to collect information and communicate with others without outside interference.

Encryption is a fundamental building block for freedom of expression, respect for privacy, freedom of assembly and association and the rights of children as enshrined in the EU Charter of Fundamental Rights and other international treaties such as the European Convention on Human Rights.

It is the foundation for the digital economy, and makes economic espionage more difficult. Encryption protects our sensitive personal data, company secrets, journalists' sources, human rights defenders and government interests.

Companies

For companies, encryption is essential since this technology plays a fundamental role in being able to trust our digital infrastructure.

All of the digital processes that are essential for businesses rely on the security provided by encryption, whether it is stocking up physical stores, a shop window in the form of a website, the efficient servicing of clients, the import of raw materials and products from anywhere in the world, the payments made by customers or the administration of taxes.

The explosion of online financial transactions and the growth of Europe's successful banking infrastructure in recent decades would not have been possible without encryption.

Companies also rely on encryption in order to protect business secrets against espionage from other companies and state hackers, as well as protecting data on stolen or lost laptops.

States

States are heavily dependent on the use of encryption to ensure the authenticity, integrity and confidentiality of information with the aim of protecting their national security.

National governments safely discuss important matters with their embassy staff abroad. They communicate with their constituencies efficiently in times of crisis, such as a pandemic.

Citizens submit tax returns online. Intelligence services encrypt state secret to protect them against interception from third states.

The army sends orders securely in order to avoid compromising military operations and the police exchange information in the course of their criminal investigations. Civil servants negotiate trade deals by sending messages that only the addressee can read. Public operators use encryption to secure access to management interfaces of pumping stations and other critical infrastructures. The list of use cases is endless.

Individuals

People need encryption to safely navigate the digital world. They order new clothes, furnitures and food on websites that are secured by the "s" in "https://" and can securely pay for them with their banking app thanks to banks' encrypted payment systems. People also catch up with loved ones far away on WhatsApp and chat with their friends over Signal messages.

They organise peaceful assemblies to advocate on encrypted Telegram groups for change and thus, exercise their human rights in the digital age. They feel relieved to know their contacts and photos are safe when they lose their phone or tablet.

Lawyers and doctors can feel confident that they abide by their confidentiality obligation when corresponding online with their clients or patients. Children benefit from encryption to keep their online activities private and safe.

Democratic society as a whole

It is not just individuals and institutions that benefit from encryption, it is our democratic society as a whole - even beyond the borders of the European Union. Some governments protect their (partially digital) elections and allow for remote participation.

Encryption is used by journalists to secure their communications and information in order to protect their sources. Marginalised groups rely on the technology to talk freely about things that are considered sensitive in society.

Human rights advocates, both in and outside of the European Union, trust encryption with their lives.

Weakening encryption will severely harm Europe

Encryption is one of the few instruments we can trust to securely navigate our digital world.

Mandating limitations on the use of encryption will come at a high cost: the loss of trust in anything we do online and increased risks to the security of our democratic society, to the economy and to our human rights.

Fundamental rights in the EU and worldwide will be endangered

Introducing limitations on the use of encryption will enable third parties (whether the police, foreign states or criminals) to have access to our confidential information.

Because individuals will be aware of the risk of third parties surveilling their online activities, they'll self-censor. This chilling effect will severely impede the exercise of rights as well as people's autonomy and selfdetermination.

Such a restriction also sets a bad precedent and will be followed in countries without respect for the rule of law or adequate legal protections. It is impossible to restrict such limitations to services offered in the European Union only.

If an intervention requires a change to the technical architecture of platforms which operate globally, such a change would be rolled out internationally - including to countries lacking the legal standards of the European Union.

Weakening encryption for European users will weaken encryption worldwide.[iv]

The economic costs of weakening encryption will pile up

Mandating limitations to the use of encryption will erode trust in encrypted communications.

This shattered trust will in turn undermine innovation and economic development. It will probably make companies that operate globally reconsider whether they want to do business in Europe.[v]

Even if they do continue to operate in Europe, users will be more reluctant to use these services, since their information is less secure against abuse by third parties. If compliance with legal obligations requires changes to the infrastructure of encryption systems, companies will need to make additional investments and costly adjustments to their products.

Mandating vulnerabilities in encryption systems also means putting companies that operate globally in a difficult position when providing their services in countries with a less adequate rule of law.

Limitations to encryption will also impede further innovation in the field of encryption.[vi]

Trust in our governments will be undermined

A government that limits the use of encryption also sends a signal to society that it does not consider the protection of fundamental rights and the security of our digital infrastructures

to be important enough. Mandating restrictions on encryption stands in complete contradiction with regulations that are supposed to protect our rights and freedoms, such as the General Data Protection Regulation (GDPR).

Finally, trust in our governments will be undermined if it becomes easier for malicious actors to alter the official communications of the government.[vii]

Security threats will increase and become unmanageable

The number of possibilities for criminals to evade government-ordered restrictions on encryption are infinite. This is why a limitation on the use of encryption can't be effectively enforced and the ones who will suffer the most are individuals trying to live their lives, companies, and governments using compromised encryption.

Requiring companies to implement a functionality that would allow law enforcement to access otherwise encrypted information (so-called "backdoors") is intentionally creating a vulnerability in the security of a system.[viii]

The installation of intentional vulnerabilities increases the complexity of the software and increases the risk of additional and unintended vulnerabilities.[ix]

Furthermore, a built-in vulnerability can be used by anyone, not solelyx by police investigators and intelligence services of a specific country.xi Sooner or later, a vulnerability that is kept secret will be

[i] From this point on this document only speaks of "use of encryption", which should be read as "the development, availability and use of encryption."

[ii] A summary of some basic concepts surrounding encryption can be found in the EDRi booklet "How the Internet works".

[iii] The original message, called "plaintext", is also a component of encryption. This is why client side content scanning, which allows third parties to read information that is otherwise end-to-end encrypted, also weakens encryption. Client-side content scanning thus undermines the fundamental characteristic where only the sender and the intended recipient are able to read the encrypted information.

[iv] The instant messaging service WeChat is offered in China as well as globally. Even though WeChat separates Chinese users from international users, the latter are subjected to surveillance and censorship by Chinese state authorities, at least when they communicated with users within China.

[v] A number of companies have expressed highly negative views about the investment climate in the Netherlands in response to the then proposed Security Act. In 2015 Dutch Telecom company Voys said "If you value your customers' privacy, don't start up in the Netherlands [...]". See https://www.voys.nl/weblog/startups-stay-away-from-the-netherlands-if-you-valueprivacy/

[vi] A concrete example is "forward secrecy", a technique in which keys are destroyed after use. Thus, keys that are stolen cannot be used to intercept communications sent either earlier or later. If manufacturers are required to include an extra key so that the government can unlock communications, the disadvantages of "forward secrecy" are lost.

[vii] For example, a way to alter official communications of governments is to carry out a man-in-the-middle attack (MitM). A MitM attack is a cyberattack where the attacker secretly inserts themselves between two parties who believe that they are directly communicating with each other. For instance, Diginotar was a certificate authority, issuing certificates for the Dutch government. A certificate authority acts as a trusted third party certifying secure connections between two entities. In 2011 the company saw a near total compromise of its systems. An attacker issued a wildcard certificate that was subsequently used by unknown persons in Iran to conduct a man-in-the-middle attack against Google services. Once the certificates used by the Dutch government was revoked or marked as untrusted by browsers, it was difficult to access services such as the public identity management platform DigiD and the Tax

found and abused by malicious users and rogue governments willing to crack down on political dissidents, human rights defenders and journalists, etc.

Once built, such weaknesses in software can haunt us for decades. A number of serious vulnerabilities discovered in security software in recent years were ordered by governments decades ago.

That's why supporting and guaranteeing the use of encryption is of paramount importance today in Europe.[xii]

and Customs Administration website. Another famous example is the hack of the lawful interception facilities of Vodafone in Greece ("The Athens Affair"). It enabled the eavesdropping of over 100 politicians and other people of interest. This is yet another example with a high impact on national security and which would have been prevented by the application of end-to-end encryption.

[viii] **See also "Keys under Doormats" report by fifteen renowned cryptographers, amongst them Ross Anderson, Matt Blaze, Whitfield Diffie, Matthew Green, Ronald L. Rivest and Bruce Schneier.**

[ix] **In the 1990s, the American government introduced a backdoor, "the Clipper Chip", which had to be installed in all kinds of systems. Cryptographer Matt Blaze showed that this deliberate vulnerability itself contained a vulnerability. See** https://www.mattblaze.org/papers/eesproto.pdf **and** https://www.theregister.com/2020/01/27/clipper_lessons_learned/.

[x] **Equipment from the American company Cisco contained vulnerabilities installed to allow investigation and intelligence services access to internet traffic handled by these devices. This functionality contained leaks that were exploited by attackers.**

[xi] **In Greece, legal call-intercept functionality that was intended for use by law enforcement was hacked. The perpetrators illegally eavesdropped on the conversations of more than a hundred members of parliament and high-ranking civil servants. This illegal wiretapping began in the summer of 2004 and was not discovered until the following spring. A more recent example is Google's interface, which gives law enforcement and secret services access to Google's customers' data. This database of which customers were being monitored was accessed by the Chinese secret service to determine if their spies were known to the American government. A backdoor in Juniper firewall devices, inserted at the request of the NSA, was allegedly taken over by a hacking group associated with the Chinese government and used for breaching network security of Juniper's customers See** https://en.wikipedia.org/wiki/Greek_wiretapping_case_2004%E2%80%9305 and https://www.datacenterknowledge.com/security/juniper-breach-mystery-starts-clear-new-details-hackers-and-us-role

[xii] **The restrictions on the export of encryption technology in the 1990's are still causing problems today. Even though the restrictions were lifted almost two decades ago, the weak encryption code was, for understandable reasons, never removed – it was forgotten. In 2015 it became clear that malicious hackers could exploit the forgotten code. Investigators discovered two vulnerabilities, known as FREAK and LogJam, whereby systems could be fooled into using the weak encryption, which, with the speed of modern computers, is almost trivially easy for attackers to decrypt.**

“By keeping such vulnerabilities [in computer systems] open, or even creating them, those resorting to hacking may contribute to security and privacy threats for millions of users and the broader digital information ecosystem”-

Report of the Office of the United Nations High Commissioner for Human Rights, 2022

Mass surveillance. Random Censorship. Content Restrictions.

Companies and governments increasingly restrict our freedoms.

–

DONATE NOW:

https://edri.org/take-action/donate

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us
Rue Belliard 12
1040 Brussels
Belgium

Follow us
Twitter
Facebook
LinkedIn
Youtube

European Digital Rights (EDRi) is the biggest European network defending rights and freedoms online. We promote, protect and uphold human rights and the rule of law in the digital environment, including the right to privacy, data protection, freedom of expression and information.

www.edri.org