EUROPOL

EUROJUST

Second report of the **observatory function on encryption**

Joint report

JOINT REPORT
Europol and Eurojust Public Information

Contents

List of abbreviations

AES – Advanced Encryption Standard

CDN – Content delivery network

CEO – Chief Executive Officer

DA – District Attorney

DNS – Domain Name System

DoH – DNS-over-HTTPS

DoT – DNS over TLS

E2EE – End-to-end encryption

EC3 – Europol's European Cybercrime Centre

ECHR – European Court of Human Rights

FBI – Federal Bureau of Investigation

FHE – Fully homomorphic encryption

GAN – Generative adversarial network

HTTP – HyperText Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

IETF – Internet Engineering Task Force

ISP – Internet Service Provider

IP – Internet Protocol

LEA – Law enforcement authority

M3 – Mobile Magic Mirror

MEC – Multi-access edge computing

NGO – Non-governmental organisation

NISQ – Noisy intermediate scale quantum

NIST – National Institute of Standards and Technology

PHE – Partially homomorphic encryption

PGP – Pretty Good Privacy

RFC – Request for Comments

RSA – Rivest-Shamir-Adleman
SHE – Somewhat homomorphic encryption
TLS – Transport Layer Security
VPN – Virtual Private Network

1 Executive summary

Encryption remains an ongoing topic of debate across the globe, without easy or straightforward solutions. Since the completion of the research of the first report of the observatory function, new statements and responses from different perspectives involved in the debate have been introduced, as well as different developments which may further complicate the landscape of encryption and its role in the investigation of criminal cases. This report aims to provide an update based on developments that occurred after the first report, or developments which are relevant but were not included in the first report for other reasons. The report contains an update on relevant statements or propositions made with respect to how law enforcement can potentially cope with encryption and its related challenges.

These challenges relate to technological developments as well as to the legal landscape. The first part of the report focuses on the legal challenges. Challenges in the legal landscape occur in part because of the application of general legal provisions. At the same time, criminal defendants contest specific legal provisions in courts, especially when it concerns legal obligations for suspects to hand over the encryption key or data in an unencrypted format.

The subsequent part of the report focuses more on challenges related to technological developments or challenges related to policies and business models that technology companies have introduced. Criminal usage of encrypted communication mobile devices is a recurring obstacle in investigations, ranging across the different crime areas. Such devices provide criminals with a manner of communication which allows them to circumvent law enforcement means of interception. The approach to encryption by technology companies, including social media companies, has also introduced and continues to introduce challenges for criminal investigations. Especially when companies use E2EE, ensuring they will also not have access to the data, and as such no means of assisting law enforcement to lawfully access electronic evidence.

Developments such as homomorphic encryption have been suggested to offer an alternative access to encrypted electronic data to law enforcement, but at the same time also seem to be accompanied by concerns. And while the topic of encryption continues to find itself in the spotlight, criminals may use alternative methods ancillary to encryption to hide their criminal activities, such as steganography. There are various developments within the field of steganography that could potentially impact the work of law enforcement. As the field of steganography rapidly develops, law enforcement is likely to be a step behind when implementing countermeasures. Yet it is not all bad news, for it can also create some opportunities for law enforcement agencies.

Other relevant elements included in the report pertain to changes to the Domain Name System (DNS), quantum computing and 5G. These developments demonstrate the diversity of encryption-related challenges for law enforcement with respect to criminal investigations. Through this report, therefore, Europol and Eurojust hope to illustrate how current challenges combined with ongoing technological developments lead to more complicated situations in the future. To respond to these challenges, insight into the developments as well as cooperation are essential.

As recognised in the first edition, this report functions as an invitation to relevant stakeholders to provide their input with regard to the identification of future developments. It is clear that law enforcement is facing challenges because of criminal abuse of encryption, but also as a result of other (technological) developments. Much of the insight into and knowledge about such developments comes from external stakeholders, whereas law enforcement can then make the translation into how such developments can influence or otherwise impact their work. In facing the described challenges, it is essential to not only cooperate with other law enforcement agencies but also with both the private sector and academia. It is certain that in order for law enforcement to try to keep up with criminal activities, it is necessary to continue investing in training and capability.

2 Progression of the encryption debate

At the end of 2018, Levy and Robinson wrote an essay aiming for a more informed exceptional access debate. Such an informed debate required more attention to detail and the inclusion of such details as part of the discussion, in particular with respect to lawful access to commodity end-to-end encrypted services and devices. "Without details," they state "the problem is debated as a purely academic abstraction concerning security, liberty, and the role of government[1]."

One proposal introduced by Levy and Robinson is to silently add a law enforcement participant to a group chat or call. From the perspective of technology companies and civil society organisations, such an introduction of a ghost participant is problematic. The adversaries of the idea pointed out that this solution is nothing more than an attempt at mandating an encryption backdoor, bringing security and privacy risks along with it.

Those who criticise the proposal acknowledge law enforcement's need to intervene. This would be on occasions where there is a legitimate reason for such action, and when it does not undermine public trust or security. However, critics perceive this specific approach as a covert way of undermining end-to-end encryption (E2EE). There is also a set of technical challenges mentioned, taking WhatsApp as an example. The first one is the need to convert the one-to-one conversation into a group chat with the ghost participant as a third person. The second one is an issue perceived from the user experience perspective. The ghost participant would have to falsify the security code necessary, and then the conversation's keys would have to be changed without the knowledge of the original participants since the notification about it would have to be suppressed. The result of those activities, according to the critics, would be a serious decrease of trust towards the service provider. The third challenge frequently mentioned is potential abuse by criminals of the "ghost" feature[2].

The debate continues as Attorney General William Barr stated during a speech how "In the world of cybersecurity, we do not deal in absolute guarantees but in relative risks," and goes on to question "whether the residual risk of vulnerability resulting from incorporating a lawful access mechanism is materially greater than those already in the unmodified product". According to Schneier, this changes the debate because the US government acknowledges that certain interventions do lead to a decrease in security. Such an acknowledgement, according to Schneier, leads to the opportunity to finally have a "sensible policy conversation[3]". This acknowledgement is important especially as this introduces an openness to the debate which is very much needed to come to actual solutions.

3 Current legal landscape to address encryption in criminal investigations

In the first report of the Observatory Function, it was explained that law enforcement authorities (LEAs) can handle encryption in two main different ways: attacking encryption and bypassing encryption. Attacking or breaking encryption would entail, for example, LEA applying brute force, installing tools or performing a lawful intercept. Bypassing encryption can be done by requesting/ordering the unencrypted data or access key to be handed over.

Below, an overview is given of the legal provisions applied by Member States when attacking encryption. Most countries use general legal provisions.

MEMBER STATE	LEGAL PROVISIONS
Austria	General provisions
Belgium	Article 39bis Code of Criminal Procedure (network search) Article 89ter Code of Criminal Procedure (sneak and peek in computer systems) Article 90ter Code of Criminal Procedure (legal hacking)
Bulgaria	General provisions
Croatia	Article 224 to 232 Criminal Procedure Act (searches)
Czechia	Section 113 Code of Criminal Procedure
Denmark	Sections 780-781 Administration of Justice Act (interception of communications) Sections 793-794 Administration of Justice Act (searches)
Estonia	§ 83 Code of Criminal Procedure (inspection and inquiries to electronic communications undertakings) § 91 Code of Criminal Procedure (searches) § 1265 Code of Criminal Procedure (covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things) § 1267 Code of Criminal Procedure (wire-tapping or covert observation)
Finland	No
France	Article 230-1 to 230-5 Criminal Code (deciphering) Article 706-102-1 to 706-102-7 Criminal Code (GOVWARE)
Germany	Sections 94, 98 and 102 Code of Criminal Procedure (stored data) Section 100a, para 1 Code of Criminal Procedure (real-time interception - source interception enabling access to unencrypted data) Section 51 para 2 new Law on the BKA (real-time interception - terrorism prevention)
Greece	Article 258 et seq. Code of Criminal Procedure
Hungary	Sections 231 and 232 Code of Criminal Procedure
Ireland	General provisions - where the devices or accounts, etc., are accessed on the basis of a legal authority such as a search warrant, the investigators may utilise any means to gain access and give effect to the provisions in the warrant
Latvia	Section 179 Criminal Procedure Code (searches) Section 186 Criminal Procedure Code (seizure) Sections 159-161 Criminal Procedure Code (inspection) Sections 193-194 Criminal Procedure Code (expert examination)

	Sections 218-220 Criminal Procedure Code (control of data)
Lithuania	General provisions
Luxembourg	General provisions
Poland	Article 19 §7 Police Act (request for the use of hacking techniques)
Portugal	General provisions
Romania	Article 138 Criminal Procedure Code (access to computer systems)
Slovak Republic	General provisions
Slovenia	General provisions
Spain	Genera provisions - pursuant to several technological measures that are regulated in the Criminal Procedure Code, the use of any technique to decrypt that can be audited and does not involve physical violence on a person is allowed Article 588septies (b) Criminal Procedure Code (remote search)
Sweden	General provisions
Netherlands	General provisions
UK (England and Wales)	General provisions - if items have been lawfully seized, the police have the power to undertake an examination that may involve damage to or destruction of the item
UK (Scotland)	Various provisions in Regulation of Investigatory Powers Act 2000 Various provisions in Regulation of Investigatory Powers (Scotland) Act 2010 Various provisions in Investigatory Powers Act 2016

Table 1: Overview of Member State encryption laws

3.1 The legal obligation to provide access keys and the *nemo tenetur* principle – legal landscape and case law

Besides attacking encryption, law enforcement and judicial authorities can also try to bypass encryption by requesting/ordering the unencrypted data or access key to be handed over. There are two ways in which this handover might be possible: a handover by the suspect or a handover by a third party who has access to the unencrypted data, such as a service provider or a third person who knows the access key.

Unless this handover happens voluntarily, successfully receiving the requested information will however very much depend on the existence and effectiveness of legislative possibilities, compelling a suspect or a third party to hand over the key or data. Where there is little controversy and disparity about the obligatory handover by third parties, the situation is much less straightforward as regards the obligatory handover of the access key by a suspect. This obligation for the suspect is namely considered by many as being irreconcilable with a person's right not to incriminate themselves (*nemo tenetur* principle). This is the reason why only a few Member States have a legal provision compelling a suspect to hand over the access key or (assist police to get access to) the data in an unencrypted format. Moreover, there are increasingly more cases being brought to court where a violation of the *nemo tenetur* principle is alleged because the defendant was obliged by law to provide their password to the police or their biometrics (in this case, fingerprint) were used against their will to unlock a device, thereby giving access to the data.

3.2 Legal provisions compelling a suspect to disclose access keys or to provide data in an unencrypted format

Currently, only five Member States have a legal provision compelling a suspect to hand over the access key or (assist police to get access to) the data in an unencrypted format. In the other Member States, such a provision is considered to conflict with the *nemo tenetur* principle. Belgium, France, Ireland and the UK currently have specific legal provisions that compel the suspect to provide the authorities with an access key, produce the data in an unencrypted format, or enable authorities to access the data. In Croatia, under the general provisions of the Criminal Procedure Act regulating searches, everyone (thus including a suspect) can be compelled to provide authorities with access to an electronic device he/she is using or of which he/she has the means of access.

MEMBER STATE	LEGAL PROVISIONS
Belgium	Article 88quater Code of Criminal Procedure
Croatia	Article 257 Criminal Procedure Act (searches)
France	Article 434-15-2 Criminal Code
Ireland	Section 48 Criminal Justice Theft and Fraud Offences Act 2001 Section 7 Criminal Justice Offences Relating to Information Systems Act 2017
UK	Part III Regulation of Investigatory Powers Act 2000 Section 49 Regulation of Investigatory Powers Act 2000

Table 2: Overview of laws compelling a suspect to disclose access keys or to provide data in an unencrypted format

3.3 Case law related to the legal obligation for a suspect to disclose the access key or use of biometrics to get access to unencrypted data

Since the implementation and application of these legal provisions, a number of cases have been brought to court by persons who provided their password to the police in the course of an investigation and claimed that their rights to silence and non-self-incrimination were violated.

3.3.1 Disparity of court motivations and rulings

In France, the Constitutional Council ruled that the legal provisions only allow the decryption of encrypted data and are not intended to obtain a confession of the suspect or carry a recognition or presumption of guilt. Moreover, the data, which is already stored on a server/device, exists independently of the will of the suspect. Consequently, the court ruled that no violation of the *nemo tenetur* principle had occurred. On the other hand, the Creteil Regional Court ruled that a suspect who refused to provide her phone PIN code to the police was indeed not obliged to do so because the court considered that the PIN code was not the (same as the) actual decryption key of the data being sought.

No consensus has been reached among Belgian courts either. Over recent years, there have been multiple court rulings on this topic. The courts used different motivations to underpin their rulings.

Several Belgian courts have considered the decryption order to be in violation with the right to remain silent under Article 6 European Court of Human Rights (ECHR), and the right of a person not to incriminate themselves. In 2017, one court considered it a violation because the person was coerced, under threat of a prison sentence, to tell the truth, so that police would be able to obtain incriminating evidence against him. Moreover, the court (and several other courts) made reference to the case of Saunders vs UK, in which it was stated that " [the right to not self-incriminate] does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, *inter alia*, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing". The court did not consider the provision of a password the same as the obtaining by the police of for instance blood samples under coercion, as the latter does not entail an obligation to speak under the threat of a prison sentence. Another court ruled in 2018 that the existence of an encryption key is dependent on the will of an individual and therefore does not exist independently and thus the use of coercion to obtain it is not allowed.

Similarly, in a more recent ruling, the court stated that "handing over a key" requires active and personal cooperation from the suspect. The coercive measures referred to in Saunders vs. UK can be implemented independent from the will of the suspect. The court stated that the existence of evidence "independent of the will of the suspect" is not the same as the existence of evidence "irrespective of the will of the suspect". After all, all evidence, except a confession, exists irrespective of the will of a suspect, and thus such an interpretation of the ruling is too narrow. According to the court, "existence" refers to the establishment of evidence. If evidence is established without personal and active cooperation or wills expression of the suspect, it exists independently of the will of the suspect. As the police could not have received the password without the active and personal cooperation of the suspect, the court concluded that his right to not self-incriminate was violated.

Notwithstanding the above rulings, several Belgian courts tend to accept that the decryption order is reconcilable with the *nemo tenetur* principle and the right to remain silent. Courts have motivated their rulings in a similar way as in France and stated, contrary to the courts mentioned above, that the access key and content of a mobile telephone exist independently of the will of the suspect. The existence of evidence should therefore be separated from the fact that the accused could possibly incriminate themselves. The courts further stated that the right to remain silent ensures that the evidence-gathering process is not manipulated in such a way that it would result in untruthful evidence, for example by using force or torture to obtain confessions. The force applied, i.e. compelling the suspect to hand over the key, could not result in the change of the access code or content of the telephone, which is already stored on the phone and therefore exists independently of the will of the suspect.

Other arguments used by the courts are the fact that the seriousness of the facts justified the application of the measure and the intrusiveness of the measure is less than if other investigative measures would be used to obtain the same result.

3.3.2 Use of biometric data accepted by courts in the Netherlands

Although no legal provision exists in the Netherlands to compel a suspect to hand over an access key, in some cases, the Dutch authorities allow the use of biometric data from a suspect to unlock a device, as was supported by two court rulings in The Hague[4].

In the first case, the police ordered the accused to cooperate in unlocking his telephone. After resisting when the police attempted to place the accused's thumb on his telephone, he cooperated and entered the code of his telephone. In the second case, the defendant similarly provided the PIN code of his phone to the police because he wanted to avoid physical coercion (the police would force him to give his fingerprint).

In the first case, the court ruled that no violation of Articles 3, 6 or 8 ECHR occurred. The accused was suspected of very serious acts, including the unlawful deprivation of liberty of two young children, and, at the time when his cooperation in unlocking his telephone was requested, the police had no idea about the location of the children. Therefore, the location of the children was urgently needed. In such a situation, some coercion is permitted and also necessary. The police did not appear to have acted disproportionately. The court was therefore of the opinion that the limited use of force was proportionate and lawful.

In the second case, the court also reasoned that the *nemo tenetur* principle was not violated and the police was authorised – with the permission of the public prosecutor – to forcibly take the fingerprint from the accused in order to unlock the smartphone. Such an order is comparable to the (forced) taking of fingerprints during investigations. It concerns biometric material that exists independently of the will of the defendant and that could be obtained without his cooperation (which is different in case of unlocking the phone by a password). The court also takes into account that there was a major interest in unlocking the phone (given the accused was detained for a serious criminal offence) and the infringement on physical integrity is minor. The fact that the defendant ultimately – and therefore in a certain way not entirely voluntarily – gave his password does not, therefore, mean that there was a formal default made.

4 Challenges

4.1 Encrypted communication mobile devices

One of the main challenges for law enforcement is the use of encrypted communication devices by organised crime groups. In May 2019, Europol and Eurojust coordinated operation "Icebreaker". The operation led to dismantling a highly professional and dangerous international organised crime group, involved in large-scale drug and cigarette trafficking, assassinations and money laundering. The leaders and members of this crime group used counter-surveillance and counter-intelligence measures to try to evade law enforcement authorities, as well as specialised encrypted communication devices. The authorities seized around 100 encrypted mobile phones customised for encrypted communication[5].

The market for encrypted communication providers dedicated to organised crime groups appears to be on the rise. These providers promise their customers enhanced security and privacy. These types of communication devices are attractive and can be abused by criminals as they can use them to make their communication inaccessible for law enforcement. Some of those companies providing these devices faced charges of cooperating with organised criminal groups.

The case of Phantom Secure appears to be one of the biggest, showing the impact and the scale of the use of mobile encryption tools by organised criminal groups. Phantom Secure was a Canada-based enterprise with a revenue of $80 million over its ten years of activity, according to the FBI. The company had up to 20 000 users and, according to the arrest warrant for the Phantom Secure's Chief Executive Officer (CEO), the company facilitated murders and drug smuggling to countries such as the US, Australia, Mexico, Canada, Thailand and parts of Europe[6]. During the FBI operation, the Agency seized 150 domains, 1 000 phones and shut down the enterprise. The company's CEO received a nine-year prison sentence.

The transcript of the conversation between the former CEO and an undercover FBI agent included in the arrest warrant shows some of the methods used by the company and also reveals that Phantom Secure was created specifically to facilitate drug trafficking[7]. According to the warrant, quoting Phantom Secure's marketing materials, it was operating mainly on the Blackberry handsets, adjusted by the company's technical team. The hardware and software tools responsible for external communications, such as a microphone, GPS navigation, camera, internet access and messaging applications were being removed. All of those services were replaced by the PGP and Advanced Encryption Standard (AES)[8] software, which was directing data through encrypted servers located in Panama and Hong Kong. Phantom Secure marketed its products as resistant to decryption or wiretapping[9].

The increased criminal abuse of secured mobile devices is visible across many criminal threat areas and is likely to continue[10], despite the lack of universal interoperability and relatively high costs of the device[11]. The cost varies from €1 500 to €2 800 depending on the provider and the length of the subscription[12]. The alternatives are also readily available – there are freely downloadable applications available for other types of smartphones.

The system of distributing the devices in the case of the phones provided by Phantom Secure was through strict referral – only existing clients could recommend new ones[13].

In most cases, the mobile phones in the network use Virtual Private Network (VPN) and different encryption methods[14]. Another solution is an encrypted container called vault, used for the extra protection of data stored on the phone[15].

Further, in cases of a suspected compromise, the owner of the device can remotely wipe all the data on the device, even if already in police custody[16]. The companies were also providing their customers with "duress passwords" that are alternatively called "panic" or "distress" passwords, enabling users to covertly wipe the device.

The Dutch Police managed to successfully infiltrate a criminal network and intercept the communication between the criminal members[17]. Criminals communicated with "cryptofoons" which only allowed the exchange of chat messages. The phones came from a company in the Netherlands. The Dutch police arrested the owners of the company based on charges of money laundering and aiding a criminal organisation. The Dutch Police gained access to the IronChat, used by criminals on the encrypted mobile devices, manufactured by the company named BlackBox. The devices were called IronPhones. The Police was able to intercept and decrypt over 250 000 messages[18] between criminals, who were facilitating drug production and illegal trafficking in heavy firearms[19]. The IronChat was using E2EE[20].

Two years prior to this success, the Dutch police managed to seize a server from a company named Ennetcom which facilitated encrypted communication between criminals through their Blackberries.

The top criminal groups in Ireland also operate through the use of encrypted devices. According to Irish Garda Síochána, the country's gangs, including Kinahan crime cartel, tend to replace PGP-encrypted phones regularly with new ones, each worth around €1 500. In 2018, Garda seized encrypted devices probably used in murder operations and facilitating drug trafficking[21].

Important to note is that the technology is legal, and came about as a result of human rights' concerns over privacy. As with many similar developments, however, criminals have recognised the availability of this type of legal services and are using them for illegal purposes. The high degree of security makes them particularly attractive to criminals[22].

4.2 Technology companies' policies and services

Part of the challenge surrounding encryption pertains to a matter of governance. Parallel to technological developments are policies introduced and decisions made by technology companies which influence the ability of law enforcement to access user data for the purposes of criminal investigations. Since November 2015, the District Attorney's (DA) office of Manhattan has written annual reports on the subject of smartphone encryption, following decisions by Apple and Google in 2014 to render data on their devices completely inaccessible without a passcode. In its most recent report, published in October 2019, the Manhattan D. A.'s Office demonstrates how there has been an

increase in the number of encrypted Apple devices seized by them for the purpose of criminal investigations – from 59.6% in 2014 to 82.2% in 2019[23]. While these figures focus on Apple devices, this obstacle applies to devices from other companies as well. Rene Mayrhofer, Google's Director of Android Platform Security, commented that locking out law enforcement was an "unintended side effect" of its latest security features[24].

According to the majority of the case examples provided in the report, the forensic review of the suspect's personal data communication devices plays an extensive role in investigations. Many investigators are unable to access critical data on smartphones, tablets, and laptops. The issue of inaccessibility is perceived as a "new normal" and is constantly increasing. The usual way of gaining access to the information is through the data recovery or a "workaround". The latter option is becoming more and more difficult since device manufacturers continually adopt new solutions and fixes in order to prevent the effective deployment of measures developed by LEA[25].

Federal and state courts in the US have been struggling with the dilemma of whether or how law enforcement should be permitted to decrypt seized electronic devices much the same way as Member States have (see also 3.1). The ongoing question is whether attempting to oblige a suspect to enter a passcode and decrypt their device violates suspect's privilege against self-incrimination and their presumption of innocence. A similar question arises with respect to the use of biometric data required to unlock the device. According to the statement by the federal magistrate judge in the Northern District of California, forcing an individual to provide their features to unlock the device would violate the Fifth Amendment[26]. The court argued that "unlocking [of] a phone with a finger or thumb scan far exceeds the 'physical evidence' created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence[27]".

4.3 E2EE for social media communication

The situation with respect to technology companies is exacerbated by the industry's shift towards developments using E2EE. In March 2019, Mark Zuckerberg provided his company's "Privacy-Focused Vision for Social Networking[28]". In this vision, he stated the following with respect to encryption: "People's private communications should be secure. E2EE prevents anyone -- including us -- from seeing what people share on our services." This decision has led to concerns on the side of law enforcement[29]. The potential implications could be significant.

In October 2019, FBI Director Christopher Wray stated that Facebook's proposal "would turn the platform into a dream come true for predators and child pornographers[30]". Around the same time, the US, the UK and Australia called on the platform to prevent the implementation of full encryption measures across its communication services unless the company grants LEA lawful backdoor access. However, the objectors of this proposal argue that it would have the same effect as "leaving keys under the mat" for the criminals. NGOs, think tanks and other organisations therefore responded with their own letter, encouraging Facebook not to give in to the "demands" of Australia, the UK and the US[31].

4.4 User-controlled encryption

More broadly, the introduction of user-controlled encryption is also relevant to discuss within this context of policies and services offered by companies. User-controlled encryption allows the user to have ultimate control over the encryption and decryption of their data. That is to say, the service provider will not possess the secret keys required to access the user's data. As with E2EE, user-controlled encryption makes it more complicated for law enforcement to access data for criminal investigations. Given that the service provider will not have a key to decrypt their customer's data, the requirement for third parties to hand over data to law enforcement will become more difficult, if not impossible, to be fulfilled. User-controlled encryption can therefore be associated with the "going dark" phenomenon that many law enforcement agencies have identified.

The conditions for this type of encryption are:

1) The user demands it;

2) The provider's business model does not rely on monetising the user's data;

3) The provider does not require the user's data for their services to function. Data recovery and server-side functionality are the two scenarios where providers would need to possess the ability to access their customer's data in order to perform their functions.

For data recovery to work, the provider must have a key to recover the user's information on their behalf. If user-controlled encryption was in use, then that data would be unrecoverable if the user does not have the password, PIN, or key that is needed to decrypt the information. Many users prefer having the option to recover their information. As long as this feature is present, the provider will have the ability to decrypt the user's information and therefore comply with law enforcement requests to access that data even without the user's participation.

In the case of server-side functionality, providers need to have a key to their user's data to perform their services more efficiently. For example, service providers will often store a master copy of a user's calendar on their server in order to synchronise it on multiple devices. Similarly, a user's emails are also likely to be stored on the provider's server as it holds a larger storage capacity. For these types of functions, it is crucial for the provider to have access to user data.

There are therefore certain services and applications that are more likely to embrace user-controlled encryption than others. For instance, email, enterprise messaging, calendar management, and collaborative editing are unlikely to use user-controlled in order to allow for the application of a data recovery function and to ensure that server-side functionality works effectively. However, instant messaging and audio conferencing do not have data recovery as a major feature and are therefore likely to embrace user-controlled encryption. For the moment, video conferencing is unlikely to use this type of encryption. Despite the similarity to audio conferencing, the data size of videos is so big that it can strain the capacity of a network. As a result, it requires server-side access. In the future, this

will probably change and therefore user-controlled encryption might also be adopted by video conferencing platforms.

It appears that while user-controlled encryption will certainly continue to grow, it will by no means be ubiquitous. It is likely that this type of encryption will mostly be present for data in motion.

4.5 Homomorphic encryption

A recent development in cryptography has opened the possibility for an encryption method that allows for data to be computed without compromising the privacy of that data. This method is commonly known as homomorphic encryption. Up until 2009, various online services provided Partially Homomorphic Encryption (PHE) or Somewhat Homomorphic Encryption (SHE)[32]. In 2009, Craig Gentry, an IBM employee, came up with another type: Fully Homomorphic Encryption (FHE)[33]. Although this was an important breakthrough, the huge computational capacity needed to process this type of encryption has meant that its adoption has been slow[34]. Nevertheless, its development over recent years has meant that today it is commercially viable[35]. Microsoft[36] and Google[37] have even released their own versions. The potential that this form of encryption holds has captivated the attention of many organisations and businesses alike across a variety of industries.

Similar to other forms of encryption, FHE makes use of a public key to encrypt content data. Only the individual with a matching private key will have access to the plaintext. However, what makes this encryption scheme stand out from the rest is that it allows for computations to be done directly onto the ciphertext. That is to say, no decryption is needed to process the data. This is due to its algebraic system[38].

An area that has been very keen to embrace homomorphic encryption is cloud computing. Though very practical, cloud computing can also be vulnerable as the data is mostly stored in plaintext. This is because traditional encryption methods would make it difficult for cloud providers to process the data and therefore provide its services efficiently to its customers. Given that the data is stored in plaintext, cloud service providers can be seen as unreliable when it comes to data protection. But homomorphic encryption could be the solution for cloud storage that is tailored for the protection of privacy.

4.6 Implications for law enforcement

Homomorphic encryption presents opportunities and challenges for the law enforcement community. The main advantage of this type of encryption would be the possibility to compare data with other organisations and run data analytics without compromising the privacy of that data. In this sense, FHE would be useful for strategic reports. Furthermore, in theory, homomorphic encryption has the potential to solve the tension between having strong encryption while still allowing for lawful interception. It would provide authorities with controlled access to data that would therefore mitigate the risk of that data being given to third parties[39].

That being said, there are concerns over the strength of homomorphic encryption. Though still a form of encryption, it appears to be weaker than other known encryption algorithms. This could pose a risk to the integrity of the data if an attacker were to use "the homomorphic nature of full homomorphic encryption to modify the ciphertext[40]." The vulnerability in FHE could be problematic if used for data at rest and data in transit. As a result, privacy advocates might question whether homomorphic encryption is actually a responsible solution[41]. In contrast, there is a threat that data protection supervisors may force the adoption of such encryption to existing data exchanges among law enforcement agencies, which would prove to be resource-intensive and would lead to many inefficiencies stemming from false positives, such as hits on common surnames. Finally, as mentioned above, the main area that is likely to adopt this form of encryption is cloud computing. The use of homomorphic encryption could create further obstacles for police investigators needing to access data stored in the cloud that is relevant to their investigations.

4.7 Steganography

Last year's Report of the Observatory Function on Encryption[42] identified steganography as an important development likely to have an impact on access to data for law enforcement. Steganography consists of hiding information in an innocuous cover. This would involve concealing information within another image, document, or any other file. The aim is to keep this information invisible to anyone who is unaware of its existence. Steganographic tools have been around for a while, with many of them being free and available to download. In the past, steganography was mostly used for state-sponsored Advanced Persistent Threats. However, over recent years, it has become apparent that criminals are embracing these techniques when executing their attacks[43].

Steganography is not confined to the realm of covert communications between actors wanting to hide their conversation from the world; it also plays a substantial role in the use of malware. Steganography makes it easier to conceal malware so it goes unnoticed when it enters the target system, and can be helpful to extract data so as to not alert the victim of this data being exfiltrated. Since the focus on encryption has been dominating the information security sphere, many criminals have turned their attention to information hiding as a means to achieve their aims[44]. For more information on how criminals have been using information hiding techniques, visit CUIN.org. This is a multi-disciplinary initiative supported by Europol's European Cybercrime Centre (EC3), to tackle the exploitation by criminals of information hiding techniques[45].

4.7.1 New developments and implications for law enforcement

There are various developments within the field of steganography that could potentially impact the work of law enforcement. As the field of steganography rapidly develops, law enforcement is likely to be a step behind when implementing countermeasures. Yet it is not all bad news, for it can also create some opportunities for law enforcement agencies. The following are some of the developments that have been occurring over recent years:

4.7.1.1 Mobile Magic Mirror

In 2016, a team of researchers at the University of Surrey developed a new information hiding technology that differs from its predecessors. Steganographic methods tend to hide information within the "content of a covert object or a channel[46]". However, this new technology allows for information to be disguised as online activities as opposed to the content of those activities. Essentially, information becomes embedded and goes unnoticed. This would make it harder to not only find the communication between two people but would also make it more difficult to detect whether there is communication occurring in the first place. To exemplify how this could work, the Mobile Magic Mirror (M3) project developed an App on Android that would hide information within Twitter activities[47]. The technology has now been commercialised by Crossword Cybersecurity.

4.7.1.2 Perfectly deniable steganographic disk encryption

Discrete Information Corp is developing a technology that can mask the presence of an encrypted drive on a machine[48]. The idea is to increase the safety of sensitive information through the use of steganographic disk encryption and to avoid forced password disclosure. In other words, the encrypted information would be forensically invisible. Cover systems appear completely normal, meaning there is no visible incriminating software. The development is still ongoing but in principle, it could be a potential instrument for criminal usage.

4.7.1.3 Fingerprints and steganography[49]

At Fudan University, two scientists have explored a method that uses fingerprints to hide encrypted messages. Their findings mean that it is theoretically possible to use the fingerprint databases to transmit secret messages. What sets this method apart is that it has the potential to evade detection from existing systems for spotting data that has been hidden through steganographic methods. This is because the ridge endings and bifurcations on a fingerprint are used to hide the encrypted message. A major advantage of this method, as compared to others, is the immense storage capacity that it holds even in case of the degradation of the source image. This is because of the maintenance of the polarity and location of data points (which harbour the secret). Furthermore, the method appears to be sturdy as it resists a variety of attacks. The technique proposed by these scientists is a major development for steganography as it sidesteps the traditional need to alter the pixels completely, and instead embeds the secret message in the polarity of the image; hence, masking the presence of the message.

4.7.1.4 Neural networks and steganography[50]

Steganography appears to not only be used by humans, but by machines too. A group of Stanford and Google researchers have shown how CycleGAN, a neural network, learnt to hide information covertly when performing image-to-image translation. The researchers trained CycleGAN to transform aerial images into street maps, and street maps into aerial images. The researchers realised that there were various features appearing in the aerial reconstruction that should have been suppressed when the original satellite image was transformed into a map. In other words, the original and reconstructed

images were too similar. Upon closer inspection, the researchers concluded that CycleGAN had been "cheating" by embedding the original photo into the map. It was replicating the features of the original image into the noise patterns of the map, therefore hiding the information it would later need to transform the map into a reconstruction of the satellite image. This explains why the aerial reconstruction was nearly identical to the original image. The researchers also noted that the capacity of neural networks to embed information can make it vulnerable to adversarial attacks. Attackers can take advantage of this vulnerability and create an image of their choice by altering the original image. Additionally, there is also concern that if developers are not careful and do not take proper measures, the vulnerability could mean their neural networks may be collecting personal data.

4.7.1.5 Watermarking

A research area that might be of interest for law enforcement is steganography in the form of watermarking. The latter is a process normally used to authenticate the identity or authenticity of a digital image or signal. But combining the two creates a unique opportunity for law enforcement as they can hide watermarks on crime photos using steganography. It would therefore allow for police investigators to identify whether these photos have then been altered in any way.

4.8 New encrypted DNS transports

The DNS is the internet's directory and a key point of control for internet usage. When a user wants to connect, the DNS converts the server's name to the Internet Protocol (IP) address[51]. DNS therefore enables users to access any online service or content. ISPs will often be responsible for routing users to their closest content delivery networks (CDN) based on the DNS queries, thus ensuring a more efficient delivery of content to users[52].

DNS over TLS (DoT) and DNS over HTTPS (DoH) are new protocols that have been adopted by the Internet Engineering Task Force (IETF), and are gaining popularity to transport DNS queries between endpoints and the configured recursive caching name server (resolver). They come as a response to the privacy risks that emerge from a vulnerable DNS that often leaks data. This vulnerability makes it easier for attackers to eavesdrop and tamper with DNS queries[53].

4.8.1 DNS over TLS

The DoT transports DNS queries over a TLS tunnel. The protocol allows for a secure connection to be made between the server and the client before the DNS queries and responses are transported. That is to say, DNS queries are encrypted and therefore secure. However, as not all servers support DoT as the protocol has yet to be fully implemented.

4.8.2 DNS over HTTPS

The DoH transports DNS queries over a TLS encrypted HTTP transport. Although similar to DoT in that it encrypts DNS queries, DoH goes a step further by mixing DNS queries within general HTTPS encrypted web traffic[54]. In other words, by allowing for the exchange of DNS queries and responses

over HTTPS, the DNS queries become indistinguishable from the general internet traffic[55]. Under the DoH standard, DNS requests can no longer be seen by ISPs or any other party between the user's device and the resolver.

The following table shows the main differences between the current DNS resolution and the DoH protocol:

	DNS resolution currently (and the last 20 years)	DoH protocol (Mozilla's version)
Working process	Local resolution is the default	Remote resolution with multiple servers is the default
	The user gets the nearest DNS while connecting (resolver)	The user gets the application marker's DNS (resolver) after installing the app
	The user has to only set the DNS (resolver) once in the operating system	The user has to set the DNS (resolver) for each new application
New gatekeepers + concentration	DNS traffic is spread across hundreds of thousands of servers	Four browser engines which have 90% of the market control 90% of the world's web traffic resolution
	Servers are everywhere across the world	These four browser engines are all in the same jurisdiction (USA)
	Easy to pick the server	
Privacy	User's queries can be intercepted	User's queries cannot be intercepted
	The user remains under their country's privacy regulations, law enforcement and neutrality rules	User's DNS data will be subject to the DNS (resolver)'s privacy regulation, law enforcement and neutrality rules
	User's DNS is normally supplied by a company that does not gains major financial benefits from targeted advertising	Many of the likely DNS providers earn their main income off data monetisation (and use cookies / fingerprinting)
Freedom for censorship	The user gets the DNS-based content filter mandated by the law of their country	The user gets the DNS-based content filters mandated by the law of the remote DNS (resolver)'s country
		The user's country may start mandating IP address filters as a response

Table 3: Differences between the current DNS resolution and the DoH protocol

In summary, the DoH protocol has produced three main changes in the way domain names are resolved:

1) The connection between the user's device and the name server becomes encrypted and hidden within normal web traffic;

2) Each individual application can resolve the DNS query using different name servers. This is because each browser or application can perform DNS queries directly, instead of relying on a network;

3) As the application providers can choose the name server used for the DNS resolution, they can control deployment and policy choices[56].

4.8.3 DNS over HTTPS controversy

The announcements made by Google and Firefox expressing their intentions to employ DoH, have sparked discussions regarding the advantages and problems of this new protocol. Privacy advocates have celebrated this development, highlighting how the technology ensures greater privacy for users as DNS queries cannot be "tracked, spoofed, or blocked[57]". One of the most cited advantages being: how the use of DoH can be effective to overcome censorship from authoritarian state-owned ISPs[58]. On the other hand, critics worry about the centralisation of DNS resolvers, and what this could mean for ISPs and law enforcement. Moreover, some critics would also argue that unlike E2EE that seeks to keep everyone from accessing the user's data, DoH only shifts trust from one DNS resolver owner, to another[59]. Despite the controversy, it is likely that there will continue to be a push for the adoption of DoH.

4.8.4 Law enforcement perspective

The DoH protocol can affect the judicial use of DNS query history in relation to malware investigation, lawful interception, and blocking of IP addresses linked to malware or child sexual exploitation material. It should be noted that if DNS resolution continues to be local and encrypted; LEAs will continue to access the data through appropriate judiciary requests to the ISP. However, if there is a case of a remote resolver being used for DNS resolution, the data will not be accessible to national authorities[60].

The consequences of the implementation of the DoH protocol for law enforcement include:

- The risk of losing access to historic DNS queries;
- Lawful interception becoming more complicated and problematic;
- Difficulty in accessing e-evidence for LEAs. The Cloud Act will apply due to a broader use of remote resolvers located in the US;
- LEAs' extraction of information useful for investigations may possibly be compromised if there is an implementation of a privacy policy for the DNS;
- Risk of disabling DNS-based content filters. This would include filters intended to block websites containing illegal streaming, illegal gambling, terrorist content, and child pornography among others;
- The compromise by hackers of a trusted DNS resolver would be undetectable from the outside world, and therefore harder to tackle.

4.9 Quantum computing

As identified in the first report of the observatory function on encryption, quantum computing is likely to have a revolutionary impact on encryption[61]. Indeed, it has already changed the way we look at encryption. What differentiates classical computers from quantum computers is that the former is built on binary values (0 or 1), while the latter is built on quantum bits that are a complex combination of 0 and 1 and have the ability to simultaneously be both numbers. As a result, quantum computers have the capacity to perform computations at a greater speed than classical computers, but only for certain very specific types of problem. While it is possible that such a computer will be available over the next 10 to 20 years, further research and development is still needed before a fully functioning quantum computer comes into existence. The reason it is of particular interest in the cryptographic community is that if a large enough, a functional quantum computer can be developed it will be capable of solving the mathematical problems that lie behind the most widely used current public key encryption schemes.[62]

Today, Google's 72-quibit universal quantum computer continues to be the closest we have come to this technology. However, there is a long road ahead before building a quantum computer that offers any practical advantages over classical computers. Furthermore, costs associated with building such a machine would be a limitation to their wide availability. Experts predict that it is likely that hybrid systems that combine classical and limited quantum computing functionality will appear first, before a purely quantum computer emerges[63]. In other words, such a computer would be rare.

That being said, the threat quantum computing could pose to today's encryption merits discussion. Given the speed at which a quantum computer could theoretically operate at, many of today's encryption algorithms could be rendered useless as they rely on the assumption that cracking the encryption through brute-force would be too time consuming. This is the case of Rivest-Shamir-Adleman (RSA) encryption[64], which would be ineffective in a world with quantum computers. Even "forward secrecy" could be inadequate in the face of quantum computing[65]. While it is very unlikely that quantum computers will be available for the general population in the early years of their creation, such a computer could pose a serious threat even if a few attackers have access to it.

For quantum computing, important developments took place in the second half of 2019. Several years ago, John Preskill coined the term quantum supremacy to describe the point when quantum computers become powerful enough to perform some computational task that classical computers could not do in a reasonable timeframe. The practical usage of the computational task is irrelevant, the focus is on reaching quantum supremacy as an intermediate milestone. On 23 October 2019, Google announced it had reached that stage, considered a major breakthrough. Shortly before, the news has already been discussed as a result of a previously leaked source of information. Google researchers published their findings in Nature[66].

Essentially, Google's efforts demonstrate how the company was able to build a quantum computer that can perform a task no classical computer can. In practical terms, Google's chip, which the company calls Sycamore, performed a computation in 200 seconds that would take the world's fastest

supercomputer 10 000 years[67]. The results of Google's efforts have not gone uncontested. IBM responded to the results by stating that they are able to reproduce the results using existing computational power. The relevance of that discussion has at the same time been called into question by others. As Cubitt notes, "Whether this experiment is just within reach of the world's most powerful classical supercomputer, or just beyond, isn't really the point. The term 'supremacy' is somewhat misleading in that it suggests a point when quantum computers can outperform classical computers at everything. In reality, it just means they can outperform classical computers at something[68]." Preskill has responded and defended the usage of the term. Simultaneously, he has introduced another concept to label the era he believes society will now enter: NISQ. This stands for "noisy intermediate-scale quantum." Here "intermediate-scale" refers to the size of quantum computers that are now becoming available: potentially large enough to perform certain highly specialised tasks beyond the reach of today's supercomputers. "Noisy" emphasises that we have imperfect control over the qubits, resulting in small errors that accumulate over time; if too long a computation, we're not likely to get the right answer[69]."

4.9.1 Key escrow and quantum computing

A frequently discussed approach for exceptional access is what is known as key escrow. The idea is that keys needed to decrypt data are held by a third party so that the data can be retrieved if necessary. Key escrows will often rely on public-key encryption. A threat that emerges with quantum computing is that if these public-key encryptions are not quantum-safe, adversaries could easily gain access to the key escrow system, therefore granting them access to the data that was protected by these keys.

It should be noted that given the scarcity and cost of this technology, actors who possess quantum computers will likely reserve their newly found capabilities for high-value targets. Regardless, as time goes by, the costs for breaking escrow packages will likely decrease. It is estimated that the time gap between the tech industry or academic lab and the second-place lab is only a few months[70]. Furthermore, it would be unlikely that the creation of a large-scale quantum computer could be kept in secret for long. The emergence of quantum computing is problematic for key escrows as it will force those who use this method to change their encryption, running the risk of implementing encryption that has gone through less vetting than the one today.

4.9.2 Post-quantum cryptography

There are two reasons for why a focus on post-quantum cryptography is imperative[71]. Firstly, it takes time to build secure encryption. Research is needed for a good mathematical base of what could be secure against something that does not exist yet. Indeed, this is a tall order for it is impossible to know what other new algorithms will be found in the future. Nevertheless, an early start would be beneficial. The second reason is that the threat is real, even if it exists in the future. There is concern that if a quantum computer emerges, today's encryptions could easily be decrypted if adversaries had been recording or collecting encrypted data. For this reason, it is encouraged to update systems to quantum-safe encryption[72]. There are encryption algorithms today that could be considered quantum-safe as they are able to compensate the effect of quantum computing by doubling the key size.

Organisations that deal with security-critical data should consider using these quantum-safe encryption algorithms.

Nevertheless, the US NIST is already in the second round of its competition to select a new standard for public key encryption that will be "quantum resistant[73]". The subject has advanced so fast that some such as IBM have already decided to offer products[74] that include their candidates for post quantum crypto, and Amazon already supports a post quantum cipher in TLS for those using Amazon's web service cloud to host their applications[75].

4.10 5G

A final relevant development to include, as was done in the first report last year, is 5G. The "fifth generation" of telecommunication systems, or 5G, is considered to be one of the most critical building blocks of our digital economy and society within the next decades. Described by the European Commission as a "game-changer", 5G is going to enable significantly faster data connections, exceptionally low latency and will be able to handle the increasing number of connected devices. The technology is thus going to form the basis for a number of innovative business models across multiple sectors (i.e. automotive industry, industry 4.0, e-health, logistics, energy, media and entertainment). The expectation is that 5G will have a significant geopolitical impact and is considered a crucial component for Europe to compete in the global market. The European Union has therefore taken significant steps to lead global developments towards this key technology.

Despite the many anticipated benefits of 5G, from a law enforcement perspective there are a number of challenges and concerns which we must address together with all the stakeholders involved. The relevant set of challenges pertains to the potential impact of 5G developments with respect to the ability of law enforcement officials to carry out lawful interception. These challenges centre around the availability and accessibility of information needed when conducting lawful interception.[76]

4.10.1 Network slicing

The concept of network slicing can and will impact on the availability and accessibility of information through lawful interception. Network slicing is a core feature of 5G. It refers to the slicing of a single mobile radio network into multiple virtual networks. This allows multiple virtual networks to be created on top of a common shared physical infrastructure.

Customisation of the virtual networks takes place to meet the specific needs of applications, services, devices, customers or operators. Network slicing will maximise the flexibility of 5G networks, optimising both the utilisation of the infrastructure and the allocation of resources. This will enable greater energy and cost efficiencies compared to earlier mobile networks.

To carry out lawful interception, in the future law enforcement will therefore require the cooperation of numerous network providers both at home and abroad. Whereas many will be subject to (national) regulation, there is also the potential of "private slices" held by "private third parties" that may not be

subjected to such regulation. Either way, the existence of network slicing leads to potential challenges rendering information unavailable or inaccessible to law enforcement.

4.10.2 Multi-access Edge Computing

Multi-access Edge Computing (MEC) will allow mobile phone networks to store and process contents in the vicinity of "cellular network participants" in order to achieve faster response times. As a result, terminal devices will in the future be able to communicate directly with each other without having to use the network operator's core network. This direct communication between users leads to consequences in terms of data retrieval for law enforcement.

Communication content and identifiers no longer have to be directed via central nodes, which means information may not be available or accessible for law enforcement.

5 Conclusion

The topic of encryption continues to create challenges for both the law enforcement and the judiciary community. The ability of criminals to exploit encryption and other forms of data security in their activities leads to a situation where law enforcement's ability to conduct investigations is hampered.

Several Member States have introduced specific legal provisions in their law requiring suspects to hand over a password or data in an unencrypted format. Case law over recent years however shows that there is no unanimity among courts on whether such provisions violate a person's right not to incriminate themselves.

While the debate about how to approach encryption-related challenges continues, technological developments also progress. Criminals already take advantage of encrypted communication on mobile devices, while the approach taken by technology companies through their policies and services also leads – however inadvertently – to increased problems for law enforcement in criminal investigations.

Other areas of development, such as steganography, DoH and DoT, and 5G decrease access to data for law enforcement even further, either because criminals discover ways to abuse the developments – such as with steganography – or because access becomes more complicated, such as with DNS and 5G.

All of these developments taken together emphasise the overarching problem of how to conduct criminal investigations in contemporary society, where sources of data used in the past to gather evidence are being cut off. Meanwhile, the question on how to tackle and respond to these challenges while taking into consideration and respecting the different interests at stake remains.

References

[1] I. Levy; C. Robinson, *Principles for a More Informed Exceptional Access Debate,* Lawfare, 29/11/19, [online] https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate;

[2] N. Cardozo, *Give Up the Ghost: A Backdoor by Another Name,* Just Security, 04/01/19, [online] https://www.justsecurity.org/62114/give-ghost-backdoor/; R. Schulman, *Why the Ghost Keys 'Solution' to Encryption is No Solution,* Just Security, 18/07/19, [online] https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/; P. Garcia, *U.K. proposal to 'Bcc' law enforcement on messaging apps threatens global privacy,* The Conversation, 04/07/19, [online] http://theconversation.com/u-k-proposal-to-bcc-law-enforcement-on-messaging-apps-threatens-global-privacy-118142;

[3] B. Schneier, *Attorney General William Barr on Encryption Policy,* Lawfare, 23/07/19, [online] https://www.lawfareblog.com/attorney-general-william-barr-encryption-policy;

[4] See Cybercrime Judicial Monitor, Nos 4 and 5, Chapter 3.

[5] *Operational Task Force Leads to Dismantling of One of Europe's Most Prolific Crime Groups Behind €680 Million Operation*, Europol Press Release, 22/05/19, https://www.europol.europa.eu/newsroom/news/operational-task-force-leads-to-dismantling-of-one-of-europe%E2%80%99s-most-prolific-crime-groups-behind-%E2%82%AC680-million-operation;

[6] C. Osborne, *Phantom Secure CEO pleads guilty to providing drug cartels with encrypted phones,* ZDNet, 4/10/18, [online] https://www.zdnet.com/article/phantom-secure-ceo-pleads-guilty-to-providing-drug-cartels-with-encrypted-phones/;

[7] AO 442 (Rev. 11/11) Arrest Warrant, Case 2:18-mj-00095-BAT, [online] https://regmedia.co.uk/2018/03/13/vincent-ramos-arrest.pdf;

[8] See: *First report of the observatory function on encryption*, Europol, Eurojust, The Hague, 11/01/19, p. 11, [online] http://www.eurojust.europa.eu/press/News/News/Pages/2019/2019-01-28_First-EP-EJ-Report-on-Encryption.aspx;

[9] *International Criminal Communication Service Dismantled,* FBI News, 16/03/19, [online] https://www.fbi.gov/news/stories/phantom-secure-takedown-031618;

[10] *National Strategic Assessment of Serious and Organised Crime 2018*, National Crime Agency, p.18, [online] https://nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file;

[11] D. E. Denning, W. E. Baugh, Jr, *Hiding Crimes in Cyberspace*, [in:] Information, Communication and Society, Vol. 2, No 3, Autumn 1999;

[12] - According to the FBI Arrest Warrant, "PHANTOM SECURE provides encrypted devices and service to its client-customers at a cost of approximately $2,000-$3,000 per six-month subscription." See: AO 442 (Rev. 11/11) Arrest Warrant, Case 2:18-mj-00095-BAT, [online] https://regmedia.co.uk/2018/03/13/vincent-ramos-arrest.pdf;
- According to the Dutch prosecutors' statement after the arrest of the Ennetcom owner, the devices cost around €1 500 each. See: *Opnieuw aanhoudingen voor leveren crypto-gsm's aan onderwereld,* 10/05/2017; [online] https://www.om.nl/actueel/nieuwsberichten/@98954/opnieuw-aanhoudingen/;
- The Sydney Morning Herald states in the article, that the phones provided by the Australian man, arrested by the police in 2015, could be bought "for between $2300 and $2800 for a six-month subscription. Users can then pay upwards of $1000 to extend their subscription for another six months." See: N. Ralston*, Are encrypted phones allowing criminals to get away with murder?,* The Sydney Morning Herald, 24 May 2015, [online] https://www.smh.com.au/national/nsw/are-encrypted-phones-allowing-criminals-to-get-away-with-murder-20150523-gh82gv.html;
- According to Police Professional, services provided by the IronChat costed "more than £2500 each year" of the subscription. See: T. Thompson, *Dutch police admit accessing criminal chats by intercepting encryption server,* Police Professional, 13/10/2018, [online] https://www.policeprofessional.com/news/dutch-police-admit-accessing-criminal-chats-by-intercepting-encryption-server/

- According to the Irish Examiner, and Irish Gardai, "The country's top gangs, including the Kinahan crime cartel, are replacing encrypted phones — costing around €1 500 each — "every couple of weeks", a senior Garda has said." See: *Garda concern over gang use of encrypted phones,* Irish Examiner, 12/02/2019, [online] https://www.irishexaminer.com/breakingnews/ireland/garda-concern-over-gang-use-of-encrypted-phones-903788.html;

[13] *International Criminal Communication Service Dismantled,* FBI News, 16/03/19, [online] https://www.fbi.gov/news/stories/phantom-secure-takedown-031618;

[14] *First report of the observatory function on encryption,* Europol, Eurojust, The Hague, 11/01/19;

[15] S. Topuzov, Introducing Secure Vault: One Place To Store Securely All Your Files, 6/11/17, https://blog.securegroup.com/introducing-secure-vault-one-place-to-store-all-your-files-securely;

[16] Z. Whittaker, *Smartphones 'remotely wiped' in police custody, as encryption vs. law enforcement heats up,* ZDNet, 09/10/14, [online] https://www.zdnet.com/article/smartphones-remotely-wiped-in-police-custody-as-encryption-vs-law-enforcement-heats-up/;

[17] M. van Dinther, *Politie breekt met success in op versleuteld netwerk van criminelen en noemt hete en doorbraak bij de opsporing,* de Volkskrant, 06/11/2019, [online] https://www.volkskrant.nl/nieuws-achtergrond/politie-breekt-met-succes-in-op-versleuteld-netwerk-van-criminelen-en-noemt-het-een-doorbraak-bij-de-opsporing~b9efec22/?referer=https%3A%2F%2Fwww.google.com%2F;

[18] T. Thompson, *Dutch police admit accessing criminal chats by intercepting encryption server,* Police Professional, 13/10/18, [online] https://www.policeprofessional.com/news/dutch-police-admit-accessing-criminal-chats-by-intercepting-encryption-server/;

[19] *Police have achieved a breakthrough in the interception and decryption of crypto communication,* Politie.nl, 06/11/18; [online] https://www.politie.nl/en/news/2018/november/02-apeldoorn-police-have-achieved-a-breakthrough-in-the-interception-and-decryption-of-crypto-communication.html;

[20] T. Thompson, *Dutch police admit accessing criminal chats by intercepting encryption server,* Police Professional, 13/10/18, [online] https://www.policeprofessional.com/news/dutch-police-admit-accessing-criminal-chats-by-intercepting-encryption-server/;

[21] *Encrypted Devices Found as Gardaí carry out organised crime* raids, 19/09/18, [online] https://www.irishtimes.com/news/crime-and-law/encrypted-devices-found-as-garda%C3%AD-carry-out-organised-crime-raids-1.3634342;

[22] J. Thomas, *Sold in Liverpool: The £3k-a-year mobile phone that can be wiped even if seized by police,* MSN News, 20/01/19, [online] https://www.msn.com/en-gb/news/newsliverpool/sold-in-liverpool-the-%C2%A33k-a-year-mobile-phone-that-can-be-wiped-even-if-seized-by-police/ar-BBSuQJz;

[23] *Fifth Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, District Attorney New York County, October 2019, [online] https://manhattanda.us16.list-manage.com/track/click?u=eaa622bed9a29dd4c9cf9a414&id=db2072c3e0&e=6376fda78d;

[24] L. Franceschi-Bicchierai, *Head of Android Security Says Locking Out law Enforcement Is an 'Unintended Side Effect'*, 30/01/19, [online] https://www.vice.com/en_us/article/yw8vm7/android-security-locking-out-law-enforcement-unintended-side-effect;

[25] *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, November 2017, [online] https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf;

[26] *In the Matter of the Search of a Residence in Oakland, California,* 354 F. Supp. 3d 1010, 1015–17 N.D. Cal. 2019;

[27] Ibid. at 1016;

[28] M. Zuckerberg, *A Privacy-Focused Vision for Social Networking,* Facebook, 06/03/19, [online] https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634;

[29]C. Hymas, *Facebook is threatening to hinder police by increasing encryption, warns Priti Patel,* The Telegraph, 30/07/19, [online] https://www.telegraph.co.uk/politics/2019/07/30/facebook-threatening-hinder-police-increasing-encryption-warns/;

[30] R. Satter, S.N. Lynch, *FBI director warns Facebook could become platform of 'child pornographers'* Reuters, 04/10/19, [online] https://uk.reuters.com/article/uk-facebook-security/fbi-director-warns-facebook-could-become-platform-of-child-pornographers-idUKKBN1WJ1N3;

[31] J. Lorenzo Hall, *Open Letter: Facebook's End-to-End Encryption Plans,* Centre for Democracy & Technology, 04/10/19, [online] https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans/

[32] A. Greenberg, *Hacker Lexicon: What is Homomorphic Encryption?,* Wired, 11/03/14, [online] https://www.wired.com/2014/11/hacker-lexicon-homomorphic-encryption/;

[33] A. Greenberg, *Hacker Lexicon: What is Homomorphic Encryption?,* 11/03/14;

[34] C. Crane, *Homomorphic Encryption,* hashedout, 20/06/19, [online] https://www.thesslstore.com/blog/what-is-homomorphic-encryption/;

[35] P. Leihn, *Homomorphic encryption now a reality,* CSO, 09/07/19 [online] https://www.cso.com.au/article/663776/homomorphic-encryption-now-reality/;

[36] See: *Microsoft SEAL,* Microsoft, [online] https://www.microsoft.com/en-us/research/project/microsoft-seal/;

[37] See: C. Doctorow, *Private Join and Compute is Google's free/open source tool to allow "multiparty computation" of encrypted data without decryption,* bointboint, 20/06/19, [online] https://boingboing.net/2019/06/20/sum-count-average.html;

[38] C. Crane, *Homomorphic Encryption,* 20/06/19;

[39] J. Benaloh, *What if Responsible Encryption Back-Doors Were Possible,* Lawfare, 29/11/18, [online] https://www.lawfareblog.com/what-if-responsible-encryption-back-doors-were-possible;

[40] Z. Peng, *Danger of using fully homomorphic encryption: A look at Microsoft SEAL,* Cornell University, 17/06/19, [online] https://arxiv.org/abs/1906.07127;

[41] J. Benaloh, *What if Responsible Encryption Back-Doors Were Possible,* 29/11/18;

[42] See: *First report of the observatory function on encryption*, Europol, Eurojust, The Hague, 11/01/19;

[43] *Internet Organised Crime Threat Assessment 2018*, p.27, Europol, 2018, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018;

[44] K. Cabaj. Et.al, *The New Threats of Information Hiding,* IT Professional, May/June 2018;

[45] *About CUIng Initiative,* CUIN.ORG, [online] https://cuing.org/about.html;

[46] S. Li, *New information hiding technology to be commercialised by Crossword Cybersecurity,* University of Surrey, 05.03.2019, [online] https://blogs.surrey.ac.uk/sccs/2016/03/05/new-information-hiding-technology-to-be-commercialised-by-crossword-cybersecurity/;

[47] S. Li, *New information hiding technology to be commercialised by Crossword Cybersecurity,* 05/03/2019;

[48] J. Leyden, *Russian doll steganography allow users to mask covert drives*, The Daily Swig, 10/12/18, [online] https://portswigger.net/daily-swig/russian-doll-steganography-allows-users-to-mask-covert-drives;

[49] C. Doctorow, *Steganographically hiding secret messages in fake fingerprints*, bointboint, 05/11/18, [online] https://boingboing.net/2018/11/05/data-fingerprinting.html;

[50] R. Bhagyashree, *CycleGAN learns to cheat by hiding information in generated images*, Packt, 02/01/19, [online] https://hub.packtpub.com/cyclegan-learns-to-cheat-by-hiding-information-in-generated-images/; C. Chu, et al., *CycleGAN, a Master of Steganography*, 31st conference on Neural Information Processing System, 2017;

[51] V. Bertola, *DNS-over-HTTPS Public Policy Briefing*, Open- Xchange, November 2018 [online] https://www.open-xchange.com/fileadmin/user_upload/Blog/DoH_Public_Policy_Briefing.pdf;

[52] *DNS over HTTPS- What Is it and Why do People Care,* Congressional Research Service, 16/10/19, [online] https://crsreports.congress.gov/product/pdf/IN/IN11182;

[53] Specification for DNS over Transport Layer Security (TLS), RFC 7858, IETF;

[54] L. Hay Newman, *A Controversial Plan to Encrypt More of the Internet*, Wired, 09/11/19, [online] https://www.wired.com/story/dns-over-https-encrypted-web/;

[55] DNS Queries over HTTPS (DoH), RFC 8484, IETF;

[56] DNS Queries over HTTPS (DoH), RFC 8484, IETF;

[57] *DNS over HTTPS Will Give You Back Privacy that Big ISPs Fought to Take Away*, Electronic Frontier Foundation, 28/10/19, [online] https://www.eff.org/deeplinks/2019/10/dns-over-https-will-give-you-back-privacy-congress-big-isp-backing-took-away;

[58] *DNS over HTTPS Will Give You Back Privacy that Big ISPs Fought to Take Away*, Electronic Frontier Foundation, 28/10/19;

[59] L. Hay Newman, *A Controversial Plan to Encrypt More of the Internet*, Wired;

[60] V. Bertola, *DNS-over-HTTPS Public Policy Briefing*, November 2018;

[61] See: *First report of the observatory function on encryption*, Europol, Eurojust, The Hague, 11/01/19, p. 11;

[62] Do criminals dream of electric sheep? How technology shapes the future of Law Enforcement, Europol, July 2019, https://www.europol.europa.eu/newsroom/news/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement.

[63] Princeton University CITP, *Implications of Quantum Computing for Encryption Policy*, Carnegie Endowment for International Peace, 25/04/19, [online] https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985;

[64] M. Rouse, *RSA algorithm (Rivest-Shamir-Adleman),* Tech Target, November 2019, [online] https://searchsecurity.techtarget.com/definition/RSA;

[65] K. Kwiatkowski, *Post-Quantum Cryptography in TLS*, Cloudflare, 20/06/19, [online] https://new.blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/;

[66] F. Arute, et. Al., *Quantum supremacy using a programmable superconducting processor,* Nature, 23/10/19, [online] https://www.nature.com/articles/s41586-019-1666-5;

[67] H. Neven, *Computing takes a quantum leap forward,* blog.google, 23/10/19, [online] https://www.blog.google/technology/ai/computing-takes-quantum-leap-forward/;

[68] T. Cubitt, Google and IBM are at odds over 'quantum supremacy' – an expert explains what it really means. The Conversation, http://theconversation.com/google-and-ibm-are-at-odds-over-quantum-supremacy-an-expert-explains-what-it-really-means-125827;

[69] J. Preskill, *Why I Called it 'Quantum Supremacy',* Quanta magazine, 02/10/19, [online] https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002;

[70] Princeton University CITP, *Implications of Quantum Computing for Encryption Policy*, 25/04/19;

[71] K. Kwiatkowski*, Post-Quantum Cryptography in TLS*, 20/06/19;

[72] Princeton University CITP*, Implications of Quantum Computing for Encryption Policy,* 25/04/19;

[73] C. Boutin, *NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals',* NIST, 30/01/19, [online] https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals;

[74] S. Bushwick, *New Encryption System Protects Data from Quantum Computers,* Scientific American, 08/10/19, [online] https://www.scientificamerican.com/article/new-encryption-system-protects-data-from-quantum-computers/;

[75] A. Hopkins, *Post-quantum TLS now supported in AWS KMS,* AWS Security Blog, 04/11/19 [online] https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/.

[76] Do criminals dream of electric sheep? How technology shapes the future of Law Enforcement, Europol, July 2019, https://www.europol.europa.eu/newsroom/news/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement.