The encryption paradox: fostering security by threatening security

Francesco Fidel Camera*

Abstract: The debate on encryption has become more and more heated in the last few years. The resurgence is mainly linked to the recent advent of two factors: on the one hand, endpoint encryption is increasingly becoming the default setting on every device. While, on the other, Internet Service Providers have started to broadly offer end-to-end encryption services. So, if data is now strongly encrypted and protected both in transit and at rest, it is law enforcement and intelligence agencies that pay the price by being unable to access the content of numerous communications. This problem has been named by the US government "going dark" as it compromises investigations and surveillance activities by creating sudden "black holes" of pivotal information. Although the proliferation of encryption can often represent a major hurdle for law enforcement, it is justified on the Internet by its inherent insecurity as a dense network of nodes where packets of information are transmitted uninterruptedly. Indeed, the Internet infrastructure rests the foundation of its success on the possibility of encrypting information so that it cannot be accessed by malicious actors. Hence, encryption "weakened" by the presence of backdoors (required by the government) to access data in cases of national security protection would alter an otherwise ironclad mechanism. And so, it will undermine the security of global cyber trafficking and, consequently, of (digital) human rights such as freedom of expression and information, the protection of personal data, and even the smooth functioning of the online market. This article aims to seek a solution that can reconcile the - seemingly - opposing demands at stake: the national and collective security as opposed to the security of Internet architecture - and the entire ecosystem of rights exercised within it. In conclusion, it will be argued that it is not feasible to reduce the overall level of communication privacy to protect collective security, as a further erosion of communication privacy would result in a substantial violation of individual freedom.

Keywords: Encryption; internet governance; law enforcement; fundamental rights; digital constitutionalism.

Table of contents: 1. Introduction. – 2. Encryption Technology. – 2.1. The Cryptosystem. – 2.2. Cybersecurity. – 2.3. Backdoors. – 3. Preventing "Going Dark"? – 3.1. A practical example. Apple v. FBI: The San Bernardino Attack. – 4. The essentiality of Strong Encryption. – 4.1. Everyday Life & Cyberattacks. – 4.2. Globalization and the "Least Trusted Country" problem. – 5. Encryption Workarounds. – 5.1. Lawful Access Requirement. – 5.2. Lawful Hacking. – 6. Untangling the Encryption Paradox. – 6.1. The "Golden Age of Surveillance". – 6.2. De-emphasizing The "Going Dark" Problem. – 7. Conclusions.

1. *Introduction*

The debate on encryption, after having slumbered for some time since the end of the USA's "crypto wars", has become more and more heated in the last years. In 1999, the Clinton administration's output on its essentiality in preserving the security of electronic communications in the advancing Internet was counterbalanced by the poor diffusion of encryption technology to a wide audience, due to its excessive complexity. The extensive toolkit available to law enforcement agencies and the government's close collaboration with the industrial sector resulted in a partnership used by the former to conduct pervasive interception activities[1].

The resurgence of the encryption debate is mainly linked to the recent advent of two factors: on the one hand, endpoint encryption is increasingly becoming the default setting on every device. While, on the other, Internet Service Providers (ISPs) have started to broadly offer end-to-end encryption services and store encrypted data on

* Francesco Fidel Camera is a law student at the University of Trento with a comparative background. His field of interest focuses on Information Technology law, which he explored in depth during his mobility year at NOVA School of Law in Lisbon, where he attended the courses of its master in "Business Law & Technology".

1. Eric Manpearl, "*Preventing Going Dark": A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate*, 28 University of Florida Journal of Law & Public Policy 65 (2017), available at https://ssrn.com/abstract=3068578 (last visited on November 1, 2022).

cloud systems. This means that not even ISPs have the encryption key necessary to access the information, which makes it impossible for them to cooperate with law enforcement authorities even if willing to do so[2].

In particular, the dramatic escalation of terrorist attacks since 2014 and the recent proliferation of child sexual abuse content have made it necessary to implement methods of secure communications such as end-to-end encryption in instant messaging systems or within online platforms. Encryption is also increasingly cited in public debate as a "safe haven" for terrorists and pedophiles and pointed to by law enforcement as an insurmountable obstacle in conducting investigations.

From this powder keg, at the global level, countries have started to legislate in the direction of a functional downsizing of the technical capabilities of encryption technologies. In the European Union, as fear of terrorism increased, the most affected member states including France, Germany, and the UK started calling for a policy solution to the encryption problem by signing a joint letter highlighting the most critical aspects. They denounced the lack of technical expertise and computing processing power in law enforcement agencies combined with the absence of cross-border coordination and the inadequacy of Mutual Legal Assistance in Criminal Matters Treaties (MLATs). They also criticized the ubiquitous end-to-end encryption in e-mail services and messaging applications, which the inaccessibility to pivotal information during surveillance and investigation activities derives from.

On the opposite side of these alarming initiatives, there are privacy and freedom of expression activist groups, high-tech companies, and IT specialists who argue for strong encryption to protect digital communications from inappropriate interference. However, this heated debate should not be reduced to a mere tug-of-war between national security and privacy. The overall context is much more diverse, encompassing cybersecurity and Internet global governance issues, up

2. See *ibid*.

to economic repercussions on the reputation of companies and international trade policy[3].

This essay aims to seek a solution that can reconcile the seemingly opposing demands at stake. In doing so, we will begin with a technical description of encryption to highlight the peculiarities that make this type of technology so polarizing. Then the practical impact that widely disseminated strong encryption is having on law enforcement investigations will be analyzed. The third section discusses the indispensability of strong encryption to ensure full security in information infrastructures both in everyday life and at a global governance level. Afterward, the state of the art will be used to assess the possibility of identifying alternatives to strong encryption, or alternatives that can circumvent its effectiveness if necessary. In the final part of the article, conclusions are drawn about the legal implications arising from the implementation of end-to-end encryption tools in the public and private sectors. An attempt to solve the paradox generated by encryption by contextualizing the problem of "going dark" in the larger framework of the armamentarium of law enforcement and national security agencies, will be made.

2. *Encryption Technology*

Before proceeding to the legal dimension of this discussion, it is worth describing the basic elements and functioning of this technology. A technical overview is indeed essential to fully understand the legal issues related to end-to-encryption tools, and consequently to be able to examine policies adopted by some selected countries (namely India, China, and the USA).

2.1. *The Cryptosystem*

Although encryption entered the public debate not more than thirty years ago, its use dates back to ancient times, long before the

3. Olivia Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption*, 1 University of Illinois Journal of Law, Technology & Policy 1-48 (2019), available at https://doi.org/10.2139/ssrn.3035045 (last visited November 1, 2022).

advent of computers. Numerous examples can be found in the Greek and Roman civilizations for military purposes. A more modern and well-known example might be Germany's Enigma code used during World War II to communicate between radio towers in Europe and U-boats in the Atlantic Ocean[4]. Certainly, these techniques were very rudimentary and even in the most complex scenarios, as in the last case, soon became obsolete and easy to decipher.

From the computer age onwards, encryption has shifted to the protection of electronic communications over the Internet as a mechanism to ensure the confidentiality of these. Especially in an ecosystem like the digital one where data, including access credentials and personal communications, can be intercepted by malicious actors at any time. Thus, inevitably putting privacy and business transactions at serious risk[5].

Encryption technology allows a process of encoding a text in order to make it indecipherable to those not authorized to read it[6]. Encryption is a one-way process that, while extremely easy to achieve forward, is much more difficult to carry out backward. This result is obtained through the use of a pair of algorithms selected from a series of non-reversible mathematical transformations of the encrypted text. The series of these transformations make up the so-called "cryptosystem"[7]. In the cryptosystem, the original text, known as plaintext, is turned by the encryption algorithm into its incomprehensible form, the ciphertext. It then returns to its initial form again thanks to the decryption algorithm. The operation of this pair of algorithms is driven by two keys: one for encryption and the other for decryption. Within this

4. Peter Swire and Kenesa Ahmad, *Encryption and Globalization*, 23 Columbia Science and Technology Law Review 416 (2012), available at https://doi.org/10.2139/ssrn.1960602 (last visited November 1, 2022).

5. See Gary C. Kessler, *An Overview of Cryptography* (Princeton University, November 17, 2006), available at https://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pdf (last visited November 1, 2022).

6. Manpearl, *Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate* at 77 (cited in note 1).

7. Naresh Vats, *Weak Cryptography - A Threat to National Security and Economy*, 2 Himachal Pradesh Journal of Social Sciences 212, 212 (2012), available at https://www.academia.edu/14761025/_WEAK_CRYPTOGRAPHY_A_THREAT_TO_NATIONAL_SECURITY_ (last visited November 1, 2022).

mechanism, the focal point lies in the generation and sharing of these two keys.

There are two main approaches in this respect. First, the "symmetric" encryption approach, also called "private key" encryption in reference to the encryption key, which is the same on both ends of the communication, and which is kept secret. This means that the sender will encrypt the plain text with the same key that the receiver will use to decrypt the ciphertext. In alternative there is the "asymmetric" encryption approach, in which the receiver has a public key that everyone can access paired with a secret key that only he or she knows and is used to decrypt the messages. This way, anyone interested in sending a private text will only have to encrypt it using the public key knowing that only that specific receiver can decipher it[8]. The keys are two and they are kept separately. However, they are related to each other in a mathematical way through a "one-way function"[9]. The same is true vice-versa; hence if the receiver wants to reply to the received message, he has to wrap the text with the public key of the previous sender (now a receiver) who will in turn unwrap it using their private key.

2.2. *Cybersecurity*

One of the fundamental elements in ensuring the security of a cryptosystem is the length of its keys. The number of combinations needed to identify the keys increases exponentially as the number of bits increases. Indeed, each additional bit doubles the number of possible keys, making a hypothetical attacker's job more and more difficult, as well as the required computing power of his or her equipment more and more powerful.

A demonstration of the importance of the keys' length is given by the current Encryption Law of India, enacted in 2000, which stipulates that keys may not exceed 40 bits[10]. A key with only 40 bits is extremely easy to decipher as proven by cryptographic experts: in 1996

8. Swati Tawde, *Cryptosystems* (eduCBA March 6, 2021), available at https://www.educba.com/cryptosystems/ (last visited January 19, 2022).

9. A "one way function" in computer science represents a calculation significantly easier to execute in one direction than it is to reverse. To exemplify: from x it is quite simple to derive f (x) but, conversely, given f (x) to calculate x is highly complex.

10. See India's Information Technology Act, Section 84A.

Matt Blaze demonstrated how less than five hours were sufficient to break through with no more than $400 worth of equipment[11]. Today, with the enormous technological progress, such a barrier is basically an easy job for any hacker.

However, a long key alone does not ensure the impenetrability of encrypted messages if the cryptosystem is not properly implemented or if it is deficient by design[12]. In fact, in an immaculate cryptosystem in which each attempt generates the same chance of success, a malicious actor wishing to break into the cryptosystem, will need to expedite on average half the possible attempts to decipher the key. However, most of the algorithms on which these systems are implemented are imperfect, which means that they are not able to generate keys in a totally random manner[13]. Thus, an attacker who somehow learns, for example, that there are only odd numbers in the key will see the potential combinations further halved.

For this reason, an algorithmic peer review under public scrutiny is of fundamental importance to ensure the reliability of a cryptosystem. That is why the international community has serious doubts about the encryption algorithms developed domestically by China outside of any public peer review.

The last variable to consider, as mentioned above, is the implementation of the cryptosystem. Even if equipped with long keys and proven algorithms, its implementation in a more complex informatic system increases the overall number of vulnerabilities due to the many interactions that can take place with the other elements.

2.3. *Backdoors*

An artificial vulnerability that deserves separate treatment is backdoors. They are access points deliberately created by software designers at the request of certain stakeholders, usually law enforcement and national security agencies. However, this creates a weakness

11. Matt Blaze, et al., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists* (January, 1996), available at https://people.csail.mit.edu/rivest/pubs/BDRSx96.pdf (last visited January 19, 2022)

12. Swire and Ahmad, *Encryption and Globalization* at 431 (cited in note 4).

13. See *id.* at 432 (note 23).

that can easily be exploited by originally authorized third parties[14]. The main backdoor scheme can be exemplified by the "key escrow" mechanism. The US government creates and distributes encryption keys to national tech companies, maintaining a sort of "master key" in escrow, with which the government can decipher any encrypted data[15]. It is thus possible to allow law enforcement authorities to access the content of these tools while maintaining strong encryption with sufficiently long keys. However, it must be considered that the user will necessarily have to store the keys in a data bank, holding them in escrow. Access to the keys to decrypt the suspicious communication will be granted to law enforcement or national security agencies only after obtaining a court order. While unrelated communications will remain unavailable[16]. The problem with this approach is that there is no guarantee that these access points will only be used by authorized persons for lawful activities.

Keeping encryption keys in a registry also means exposing them to a high risk of ending up in the possession of malicious actors whose intent is to harm those same companies. Indeed, the storage of keys in a centralized database creates "high-value targets" for attackers[17].

So, if, on the one hand, backdoors can facilitate surveillance and investigation activities, on the other hand, they create a security vulnerability in a pivotal sector such as technology, undermining the security of the whole technological architecture implemented by the individual country.

14. Ben Wolford, *What is an encryption backdoor?* (ProtonMail Blog, June 22, 2018), available at https://protonmail.com/blog/encryption-backdoor/ (last visited January 21, 2022).

15. See *ibid.*

16. Manpearl, *Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate* at 77 (cited in note 1).

17. Whitfield Diffie and Martin Hellman, *New directions in cryptography*, 22 IEEE Transactions on Information Theory 644 (1976), available at https://doi.org/10.1109/tit.1976.1055638 (last visited November 1, 2022).

3. *Preventing "Going Dark"?*

Messaging and e-mail applications in today's world provide encrypted communication services as a technical standard for the benefit of users, who can exchange messages in a completely secure manner thanks to end-to-end encryption. In addition, mobile devices, once locked, do not allow access to their contents to anyone who does not have the unlock key. This is due to endpoint encryption[18].

But not all that glitters is gold. If data is now strongly encrypted and protected both in transit and at rest, it is law enforcement and intelligence agencies that pay the price. Efforts made during surveillance and investigation activities risk being undermined by these sudden "black holes". In a campaign against this blackout, the FBI has begun to refer to this problem as "going dark" and the urgent need to prevent it to ensure the safety of the community.

This technological structure constitutes a serious obstacle to investigations, leaving the field open to the recruitment and organization of terrorist attacks, and to the exchange of child pornography, now increasingly relocated on encrypted platforms. As devices and apps programmed by default with encryption have become widely available on the market, the number of communications that law enforcement authorities legally have the power to intercept, but the technical inability to execute so, has expanded exponentially. The discrepancy between legal and technical power has been addressed as creating an irremediable public safety problem. As eloquently described in the words of FBI Director James Comey, "going dark" means preventing people in charge of protecting the community from accessing the evidence needed to prosecute and prevent crime with lawful authority[19].

The need to obtain lawful access to encrypted information thus becomes the last resort to solve cases that would otherwise end up being filed. As well exemplified by the case between Apple and the FBI

18. Manpearl, *Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate* at 68 (cited in note 1).

19. James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* (Federal Bureau of Investigation, October 16, 2014), available at https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy (last visited November 1, 2022).

concerning the San Bernardino (California) massacre, which made headlines for its intense dispute.

3.1. *A practical example. Apple v. FBI: The San Bernardino Attack*

On December 2, 2015, a married couple fuelled by extremist Jihadist ideologies committed a mass shooting in the San Bernardino County Department of Public Health, killing 14 people and seriously injuring 22. A few hours later, both terrorists lost their lives in a firefight with the police. Apparently not connected to any terrorist group, the FBI claimed that their indoctrination had taken place via the Internet by exchanging private messages with each other. However, the device they were communicating with was the iPhone 5C, which provided for encryption of the data on it and complete deletion after ten failed attempts to unlock it. Hence, the FBI asked the National Security Agency (NSA) to break into the phone. However, they had no success because they did not have any experience with this kind of device. Finally, the request was forwarded directly to Apple Inc. which refused to change the software to allow the FBI access to the encrypted content through a backdoor. This opposition also persisted towards a warrant issued in favor of the FBI[20].

This stance by Apple was publicly justified by its CEO Tim Cook on the basis of the unprecedented significance of such a request. Allowing the government to demand changes to any software code at will in the future would significantly compromise the protections of the Fifth Amendment[21], as computer code has already been recognized as a form of speech[22].

"What is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user?" was argued eloquently

20. Tim Cook, *A Message to Our Customers* (Apple Inc. February 16, 2016), available at https://www.apple.com/customer-letter/ (last visited January 24, 2022).

21. The Fifth Amendment to the United States Constitution affirms a number of guarantees around the due process of law, including the right to be free from coercion as to what one wants to say. The so-called "compelled speech".

22. See *Bernstein v. U.S*, 192 F.3d 1308 (9th Cir 1999).

by Tim Cook[23]. Requiring software to be modified by removing its security features means endangering the privacy and safety of all its consumers, towards whom Apple has a responsibility to ensure the maximum security of its products[24]. Hence, it is crucial to avoid an impact that goes well beyond the present case and would set a precedent that could lead to dystopian scenarios.

The FBI, for its part, argued that the refusal to decrypt the contents on the mobile phone prevented the execution of a warrant obtained through legal channels and threatened the public interest in a complete investigation of a "horrific act of terrorism"[25]. Citing as precedent *United States v. New York Telephone Co.*[26], in which the Supreme Court had ruled on a telephone company's duty to provide technical assistance in order to allow access to the phone calling record.

In the end, faced with Apple's insurmountable wall, the FBI decided to hire professional hackers from an Israeli company who used a zero-day vulnerability in the iPhone's software. After 10 incorrect tries at guessing the code, the "Bureau"[27] could disable a feature in the device that wiped data in the smartphone, and later succeed to access the encrypted content[28].

---

23. Kim Zetter and Brian Barrett, *Apple to FBI: You Can't Force Us to Hack the San Bernardino iPhone* (Wired, February 25, 2016), available at https://www.wired.com/2016/02/apple-brief-fbi-response-iphone/ (last visited January 23, 2022).

24. Romain Dillet, *Apple's Tim Cook on iPhone unlocking case: "We will not shrink from this responsibility."* (TechCrunch, March 21, 2016), available at https://techcrunch.com/2016/03/21/apples-tim-cook-on-iphone-unlocking-case-we-will-not-shrink-from-this-responsibility/ (last visited January 23, 2022).

25. *US v. In the Matter of the Search of An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, C.D.CA. February 16, 2016.

26. *United States v. New York Telephone Co.*, 434 U.S. 159 (1977).

27. In cybersecurity, a zero-day vulnerability is a security flaw of a software whose existence is unknown to the software developer. "The Zero day" is the period of time to take action, i.e. as soon as possible, so that those same vulnerabilities are not exploited by third parties.

28. Ellen Nakashima, *FBI paid professional hackers one-time fee to crack San Bernardino iPhone* (Washington Post, April 12, 2016), available at https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html (last visited January 24, 2022).

Anyway, this case between a national government and a manufacturing company marked the re-emergence of the public debate around encryption. The question of how it can be expected to carry out international and domestic defense duties if it is not possible to access the evidence needed, even if a legal title was obtained, is left open.

To better understand the impact that encryption is having on law enforcement, it may be very useful to briefly outline the history of wiretapping, through which lawful interception has been conducted in the recent past. It all began with the spread of telephones. The wiretapping practice originally consisted of placing a listening device, the wiretap, in the circuit which transmits sound waves between two phones, with the police touching a copper wire in the copper wire located between the interceptor's house and the telephone company's switch[29]. However, with the advent of optic fiber lines in the 1990s, this *modus operandi* was no longer viable as glass fiber directly connects the interceptor to his or her telephone exchange, creating a major obstacle to the investigation.

The response at the government level was to involve directly telco companies. In the U.S., the Communications Assistance for Law Enforcement Act (CALEA)[30] came into force in 1994, requiring telephone companies, telecommunication service providers and manufacturers of telecommunication equipment to implement features that allow for real-time monitoring of transmissions, to keep surveillance capabilities intact in a moment where the industry switched from copper-wire to optic fiber[31]. The result was to increase the effectiveness of remote interception and the pervasiveness of surveillance. But with a well-defined limitation in the legislation, which acted as a compromise, namely that these measures would apply exclusively to voice networks and not to internet protocol communications.

Over the years the debate around encryption has been ever arising, whilst in the judicial context, these tools have had limited use. In fact, it is thought that in the USA among the 4148 wiretaps authorized

29. See Swire and Ahmad, *Encryption and Globalization* at 420 (cited in note 4).

30. Communication Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010.

31. Wiretap Report 2015, Administrative Office of the U.S. Courts (December 31, 2015).

by state and federal courts only 13 were encrypted[32]. Nevertheless, encryption by default was not as widespread then as it is now, these statistics need to be put into context so as not to naively underestimate the problem. In fact, in the practice of law enforcement, authorities will avoid wasting time and resources in obtaining authorization to intercept encrypted communications that they are unlikely to succeed in decrypting (as suggested by the fact that only 2 out of 13 encrypted devices were successfully accessed)[33]. In such cases, the police will prefer to turn to other means of investigation. Any wiretap request will thus only fall on devices that were mistakenly believed to be unencrypted[34]. However, if we analyze the statements of police officers, the situation is reversed. In 2015, Director James Comey stated that the FBI was unable to access data on 650 electronic devices out of the 5,000 that had been seized between October 2015 and August 2016. Comey then updated the numbers to 1200 out of 2800 in the period between October and December 2016 alone[35]. This suggests that even though law enforcement authorities are frequently confronted with encryption, the results that are achieved are very poor.

4. *The essentiality of Strong Encryption*

Although it can often represent a major hurdle for law enforcement, the proliferation of encryption on the Internet is justified by its inherent insecurity[36]. If one takes a look at its very structure, commu-

32. *Ibid.*

33. See *ibid.*

34. Stewart Baker, *Steptoe Cyberlaw Podcast: The Second Annual Triple Entente Beer Summit* (LAWFARE, February 23, 2016), available at https://lawfareblog.com/steptoe-cyberlaw-podcast-secondannual-triple-entente-beer-summit (last visited November 1, 2022).

35. Tom Winter et al., *Comey: FBI Couldn't Access Hundreds of Devices Because of Encryption* (NBC NEWS, March 8, 2017), available at http://www.nbcnews.com/news/us-news/comey-fbicouldn-t-access-hundreds-devices-because-encryption-n730646 (last visited November 1, 2022). See also James B. Comey, *Keynote Address at the Intelligence Studies Project Spring Symposium: Intelligence in Defense of the Homeland* (Strauss Center Events, March 23, 2017), available at http://intelligence-studies. utexas.edu/events/item/560-isp-spring-conference.

36. Swire and Ahmad, *Encryption and Globalization* at 423-425 (cited in note 4).

nications within it are transmitted from one Internet Service Provider to another through a dense network of nodes that receive packets of information[37]. The main problem is that, unlike other types of communication such as telephone communication where the players on the field were a few phone companies, here the faced situation embodies an indefinite number of possible intermediaries whose reliability is unknown. This systematic insecurity has been overcome only thanks to the possibility of encrypting messages and transactions that might otherwise have ended up easily in the hands of malicious actors, compromising any possibility of growth of the Internet[38].

4.1. *Everyday Life & Cyberattacks*

With the advent of globalization and digitalization, the issue of cybersecurity is increasingly at the center of legislative policies to better protect information infrastructures[39]. In this renewed scenario, cryptography techniques have played a prominent role in preserving security and privacy in everyday online activities. Encryption-enabled devices are ubiquitous in our daily actions: our mobile phones, our laptop, our credit card, our car keys, and so on. Decreasing the effectiveness of these protective capabilities would put a large part of our daily activities at serious risk, making our most precious assets easy prey for malicious attacks[40].

Following the advent of computer interconnectivity, we find ourselves in a cyber dimension where the "offense" (i.e., hackers), who wants to access and exploit a cyber system, needs to be able to access from only one point. In contrast, the "defense" (i.e., the user of the system in question), must be able to repel the attack on all fronts. This phenomenon can be summarized with a basic formula: "the defense is only as strong as its weakest point"[41].

Encryption is the primary defensive tool precisely because it can defend against attacks directed from any source of communication

37. See *id.* at 424-425.
38. See *ibid.*
39. See *id.* at 453-454.
40. See *ibid.*
41. Niels Ferguson, Bruce Schneier and Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* at 5 (Wiley 1st ed 2011).

while data is in transit and specularly protects all files on encrypted devices while information is at rest, regardless of whether or not malicious actors have compromised the system[42]. Concerning authentication over the Internet, a pivotal function is played by the double key fob authentication, such as the one provided by RSA, which can prevent access to any hacker using an old key[43]. If we opt for a weakened or even forbidden encryption, the result in these cases is the exposure of each node of an unencrypted communication channel to "data in motion" cyber threats by malicious attackers. The disclosure of unencrypted files to a hacker who has gained access to a device for data at rest. And finally, the absence of encryption in the authentication procedure allows the hacker to gain access to the password and any other identifying information involved in the process[44].

4.2. *Globalization and the "Least Trusted Country" Problem*

The globalization of information infrastructures and the increasingly prominent role which the Internet has taken on worldwide have marked a prolific border transfer of information between countries and significantly impacted businesses and organizations[45]. To fully understand the importance of strong encryption in a globalized world we can refer to the so-called "least trusted country" problem[46]. This, in connection with the previous discourse according to which the resistance of a cyber system must be calibrated on its weakest link, states that if a country decreases or prohibits strong encryption, any communication which complies with its specific law will be compromised, regardless of the geographical location of the starting or ending point of the transmission[47].

42. Swire and Ahmad, *Encryption and Globalization* at 456 (cited in note 4).
43. *RSA Authentication Manager Express* (RSA.com, April 18, 2012), available at http://www.rsa.com/products/AMX/ds/11241_h9006-amx-ds-0711.pdf. (last visited November 1, 2022).
44. Swire and Ahmad, *Encryption and Globalization* at 456 (cited in note 4).
45. See *id.* at 453-454.
46. See *id.* at 457-459.
47. See *id.* at 457.

Let us take under scrutiny the situation in India and China, which we previously mentioned[48]. In India, the legal system inclines towards a categorical ban on any encryption key longer than 40 bits, which provides a derisory ceiling for current cybersecurity threats. If applied in practice, such a system could reduce the reliability level of an enormous volume of communications, as India is a crucial player in the global landscape of the sensitive data business processing industry. Regarding demographics and Internet use, the situation remains unchanged in China. Its regulation provides for the exclusive use of domestic encryption technology based on algorithms that have not undergone any international peer review, and the consequent risk of the presence of government backdoors[49]. This means that merchants operating in the vast Chinese market may be required to incorporate those algorithms into their products and services, even if they are used outside of China's borders[50].

This twofold testimony suggests a legal regime that requires only weak encryption technologies can threaten the security of communications and trade from a global governance perspective. Any communication that originates terminates, or travels through these security holes will be systemically compromised, being as secure as it would be in the hands of the least trusted country[51].

The importance of strong encryption in the international arena is as evident in the provision of legally weakened encryption as in the provision requiring backdoors. Indeed, the more countries will decide to provide unique access to their law enforcement and national security agencies, the greater the potential threats will be. Not only the ones faced by China and India but also the ones faced by any data traffic from any other nation that enters its flawed orbit.

48. See § 2.2 on Cybersecurity.

49. See Yan Luo and Eric Carlson, *China Enacts Encryption Law* (Covington, October 31, 2019), available at https://www.insideprivacy.com/data-security/china-enacts-encryption-law/ (last visited November 1, 2022).

50. See Swire and Ahmad, *Encryption and Globalization* at 458 (cited in note 4).

51. See *ibid.*

5. *Encryption Workarounds*

In this chapter, an attempt will be made to assess the feasibility of ways around encryption without diminishing its strength. In the first half, it will be assessed whether it is possible, according to the current state of technology, to assume that legal access can be left open to law enforcement without compromising overall cyber security. And in the second half, it might not be better to leave the IT architecture untouched while evaluating alternative techniques to be able to read the content of encrypted data traffic.

5.1. *Lawful Access Requirement*

As we have already addressed in the section on backdoors, imposing on tech companies an access route for government agencies, poses a serious risk to the technological infrastructure of the country in question. This is true even if such imposition is made in compliance with legal procedures. And the more dependent a country is on cyber-infrastructure, the greater said risk will be.

The reason is precisely the difficulty in keeping these portals secret and therefore in the hands of the "good guys" only. Indeed, there is a wide range of potential access seekers, ranging from the attackers who want to exploit the vulnerabilities economically or politically, to "white hat" hackers whose goal is to identify security gaps to be revealed to the creators or the public, to get richer or enhance their reputation[52].

In addition to security issues, one should not underestimate the strong impact that the imposition of lawful access to private companies could have on the market. Ensuring full confidentiality of communications has become one of the main features of any electronic device, as well as one of the differential factors valued in advertising campaigns[53]. What customer would want to buy technological goods or online services from a country whose government can access the

52. See *id.* at 460.

53. See Kif Leswing, *Apple is turning privacy into a business advantage, not just a marketing slogan* (CNBC, June 7, 2021), available at https://www.cnbc.com/2021/06/07/apple-is-turning-privacy-into-a-business-advantage.html (last visited November 4, 2022).

content of his or her communications and transactions without any problems? This would inevitably affect the market share of its companies and the transit of information from the rest of the world with irreparable damage to the national economy[54].

Potential threats might also regard intellectual property rights. Cyber espionage and cybercrime practices, which have been on the rise in recent years, would be exacerbated by intentionally debilitated computer systems[55].

However, it should be borne in mind that technological progress has made available various techniques that allow lawful access to the government without diminishing the security of the cryptosystem. In this section we will review some of the most promising ones:

1) *Key Escrow System*. The key escrow is a method with which an encryption key is stored in an escrow system tied to the original user and subsequently encrypted for security purposes[56]. So that access is preserved in case the key is forgotten or permanently lost, as in the case of the death of its owner. In this way, the government or an authorized third party remains in possession of the key and can use it following a lawful process.

2) *Mandatory Biometric Encryption*. Following this approach, the objective is twofold; on the one hand, to further strengthen encryption by requiring device manufacturers to provide a biometric lock such as a fingerprint or retinal image[57]; on the other hand, to allow law enforcement to obtain a coercive unlock as, unlike a password, it would not constitute self-incriminating testimony[58]. As a matter of case law, the discriminating factor is whether there has been a mental activity on the part of the suspect to communicate a fact or

54. See Manpearl, "*Preventing Going Dark": A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate* at 82 (cited in note 1)

55. See *id*. at 82-83.

56. See Zach DeMeyer, *What is Key Escrow? - Store Cryptographic Keys* (JumpCloud, April 2, 2019), available at https://jumpcloud.com/blog/key-escrow (last visited November 4, 2022).

57. See Paul Rosenzweig, *Encryption, Biometrics, and the Status Quo Ante* (Lawfare, July 6, 2015), available at https://www.lawfareblog.com/encryption-biometrics-and-status-quo-ante (last visited November 4, 2022).

58. See *Fisher v. United States*, 425 U.S. 391, 409 (1976).

information, whereas this does not apply to physical evidence, such as fingerprints[59].

3) *Split Key Encryption*. This type of encryption represents a very advanced technique through which encryption keys are separated and carefully stored by a plurality of trusted actors who will necessarily have to cooperate with each other in order to unlock access to the set of keys[60]. It runs with the information that can be further secured by encapsulating them in other encrypted data[61]. The work of malicious attackers is thus made extremely complex since they will necessarily have to obtain all the keys according to a cumbersome process[62].

4) *Cryptographic Envelopes*. The cryptographic envelope is so called because it traces the mechanism of a normal envelope. Here, the recipient's address is given by its public key with the message being sealed using cryptographic techniques. Once it is sealed, the corresponding private key, possessed only by the addressee, must be used before it can be opened[63]. Through this method, the encryption key of the device's drive is located inside a cryptographic envelope, so that the drive can be unlocked either by typing in the password held by the user or, alternatively, by opening the cryptographic envelope. The latter is forwarded to the same entity that uses the public key, which encrypts the information and seals it using strong encryption[64]. To surround the process with additional guarantees, it is possible to imagine storing the cryptographic envelope within other envelopes[65]. The operating mechanism, in this case, would be to send the envelope to the law enforcement authority using its public key and then insert it in another cryptographic envelope to be sent this time to the device

59. See *Schmerber v. California*, 384 U.S. 757, 764 (1966).

60. See Geoffrey S. Corn, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data* (SSRN Electronic Journal, July 13, 2015), available at https://doi.org/10.2139/ssrn.2630361 (last visited November 1, 2022).

61. See *ibid.*

62. See *ibid.*

63. See Matt Tait, *An Approach to James Comey's Technical Challenge* (Lawfare, April 27, 2016), available at https://www.lawfareblog.com/approach-james-comeys-technical-challenge (last visited November 1, 2022).

64. See *ibid.*

65. See *ibid.*

manufacturer, so that neither entity can unilaterally decrypt the device without cooperation.

Ultimately, if we decide to go down the route marked by these law enforcement techniques to access information, it becomes possible to keep surveillance capabilities intact during investigations in coexistence with a strong level of encryption in the technology sector. If nonetheless, the cryptosystem remains unscathed in its protection, the increased structural difficulties of the overall cyber architecture significantly intensify the risk of creating additional vulnerabilities that could be exploited by malicious attackers[66].

For this reason, many scholars believe that a lawful access requirement should be denied. However, they also claim that this denial would not leave law enforcement agencies groping in the "dark". According to this vision, law enforcement agencies should be afforded additional resources and capabilities in conducting investigations. A strengthened investigative capacity would allow them to obtain the information they need for national security. In this sense, an interesting alternative could be represented by lawful hacking[67].

5.2. *Lawful Hacking*

Another viable option is for law enforcement agencies to legally exploit existing vulnerabilities in software to get all the information they need to carry out investigations. A previously created backdoor would not be needed. This category includes a wide range of techniques, varying in complexity, which turn out to be about the same as those used by hackers[68]. Such as spear-phishing, through which a social engineering method is used to obtain the encryption keys of

66. See The Heritage Foundation, *Encryption And Law Enforcement Special Access: US Should Err On Side Of Stronger Encryption - Analysis* (Eurasia Review, September 6, 2015), available at https://www.eurasiareview.com/06092015-encryption-and-law-enforcement-special-access-us-should-err-on-side-of-stronger-encryption-analysis/ (last visited November 4, 2022).

67. See Steven M. Bellovin, Matt Blaze, Sandy Clark and Susan Landau, *Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet*, 12(1) Northwestern Journal of Technology and Intellectual Property, available at https://doi.org/10.2139/ssrn.2312107 (last visited November 4, 2022).

68. See Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption* at 33 (cited in note 3).

specific targets and hence decrypt their communication[69]. Another highly used option in practice is the so-called "watering hole strategy". A malicious actor takes control of a website to send surveillance malware to all users when they log in[70].

The shared feature in all these examples is that law enforcement agencies can use means of interception for circumventing encryption without undermining the security of the cryptosystem, and of the Internet more generally, in any way. Furthermore, if lawful hacking becomes established as a default practice, rather than government-mandated encryption backdoors, the whole civil society, or specifically certain social collectives would avoid the danger of indiscriminate mass surveillance by the public authorities[71].

However, the legalized use of hacking techniques by the government does not come without raising several legal and ethical dilemmas. From a legal perspective, it must first be determined whether law enforcement agencies must first have a warrant issued by a judicial authority to proceed. Only in this scenario, one could imagine a fair use of government surveillance power while respecting the reasonable expectation of privacy of any suspect.

On the ethical front, a major stumbling block is the responsibility of the third parties with which the government contracts to perform such tasks. It is in fact customary for national governments to hire private companies that specialize in performing highly technical tasks. The risk of such a system is that it might lead to anti-competitive conduct, damaging the internal functioning of the market and requiring competitors of a given business to sabotage its products[72].

Another problem on the ethical side is whether the government has a duty to inform companies of the cyber vulnerabilities it has discovered and exploited. For example, if new software updates that are about to be launched contained vulnerabilities that hackers would be able to exploit, it would be in the government's interest not to alert the company. Surveillance activities would be carried out with no

69. See *ibid.*

70. See *ibid.*

71. See Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption* at 36 (cited in note 3).

72. Swire and Ahmad, *Encryption and Globalization at 37* (cited in note 37).

interruption[73]. The ability of law enforcement agencies to infiltrate private companies' computer systems may encourage them to invest more in cybersecurity. An increasingly secure ecosystem would in turn be created. However, in the long run, such an outcome would also make it increasingly difficult for the government to take advantage of vulnerabilities to lawfully exploit[74]. Finally, not every country has wide economic resources, (especially in IT) to be able to conduct these difficult operations and to employ private companies on a permanent basis.

6. *Untangling the Encryption Paradox*

The entire discussion underlying this essay was played out on the fine line between the need for a comprehensive law enforcement investigation and the need for a secure Internet architecture. In this difficult balancing act between fundamental rights, a perfect reconciliation is not possible. In fact, either a secure cryptographic system is ensured from the ground up, capable of guaranteeing full protection of personal data and ensuring effective freedom of expression without any constraints; or it is decided that the door should be left open for government authorities, so they can best protect public safety by having full access to all necessary information. The solution that untangles the "paradox" created by encryption must be found. The preferred solution should be capable of ensuring global security but at the same time not threatening collective security. The important thing, however, when balancing rights of fundamental importance, is that their core is preserved intact. Following this path, it is impossible to secure human rights on a network that is insecure by design without the presence of strong encryption. On the other hand, as we shall see below, as far as investigations are concerned, simply not having access to encrypted data does not mean groping in the dark. Tilting the balance in favor of privacy is then preferable.

73. See *ibid.*
74. See *id.* at 38.

6.1. *The "Golden Age of Surveillance"*

For years, law enforcement agencies have based their investigative activities on wiretapping techniques and easy access to stored records, which with the switch from "telephone" to "digital" surveillance under the banner of strong encryption have been rendered futile. Simply accessing suspicious communications does not allow any valuable insight if the data transmitted are encrypted without the possibility of decryption. This loss of pervasiveness in surveillance was emblematically described as "going dark" for law enforcement agencies, underlining how the inability to access this key information was such that investigations were permanently compromised. This conflict, which has been dormant for years following the end of the "crypto wars" in 1999, has returned to ignite public debate with strong encryption becoming the global technological standard.

Nevertheless, this aspect is only one side of the coin. The conflict must be contextualized within the broader framework of technological progress. Naturally, cryptography can create serious obstacles to investigations, but these obstacles are not insurmountable. On the contrary, surveillance capabilities of governments in the data-driven society have increased considerably, to the extent that some authors have spoken of a "golden age of surveillance"[75]. In three main areas, law enforcement agencies are now equipped with the largest surveillance capabilities ever seen:

1) *Location Tracking*. Tracking devices are so much a part of our daily lives that they have become essential for most of our actions. For many people, the mobile phone - the tracking device par excellence - is almost an extension of the body. In such a context, it is possible to trace the movements of a suspect at any time. It is now possible to verify whether he or she was at the scene of the crime at the time it took place, or to check the veracity of his or her alibi. For law enforcement, the mobile phone has become the most efficient of bugs. It eliminates the risk of having to place a physical tracker device on the suspect's person or property[76]. This is made possible by the operation of the

75. See also Swire and Ahmad, *Encryption and Globalization* at 466 (cited in note 4).

76. See *id*. at 466-467.

wireless network of telephone companies, which need access to the location of the customer at any given time in order to transmit calls to that specific phone[77]. Law enforcement agencies can retrieve this data and use it for the purposes of their investigations. While it is true that smart criminals will try to equip themselves with untraceable devices (such as prepaid mobile phones) to carry out their criminal activities, several states impose strong limits on the circulation of such devices. In addition, it should be considered that the larger the criminal circle, the more difficult it will be for each of its members to follow the same strict precautions to avoid any possible tracking activity[78].

2) *Contacts Information*. A category closely linked to the previous one is the data linked to the contacts that each subject creates through the various Internet platforms. In fact, once the police know the identifying details of a subject, they can easily trace the remaining members of a criminal organization or potential co-authors of the crime in question[79]. And, through these, further redefine the connections between them.

After the rise of Web 2.0 and online social networking[80], law enforcement agencies are able to create the "2Social Graph", or "the global mapping of everybody and how they're related"[81]. This is of paramount importance during the investigation activities because identifying the parties involved is often more useful than accessing the actual content of communications. Indeed, it allows us to expand the overall picture by adding new targets in a virtuous circle and hence enables us to better plan and direct the work needed.

3) *Digital Dossiers*. An average laptop today can hold a huge amount of information, much of which is personal data and, therefore, highly valuable for investigation purposes. However, the fact that these devices are equipped with endpoint encryption, and thus probably

77. See *ibid*.

78. See *ibid*.

79. See *id*. at 468.

80. The Web 2.0 can be seen as a second phase of the web, marked by a participatory culture that promotes the socialization among users and their direct contribution to the creation of online content.

81. Brad Fitzpatrick and David Recordon *Brad's Thoughts on the Social Graph* (LiveJournal, August 17, 2007), available at http://bradfitz.com/social-graph-problem/ (last visited February 3, 2022).

inaccessible, does not mean that those assets are necessarily lost. In a data-driven society and economy, there are many other computers, and databases, in which way more detailed records of a person's profile are stored. The reference is to records held by government agencies, banks, hospitals, data brokers, online advertisers, and many other record holders[82]. The combination of all these profiles, unthinkable until a few years ago, is able to generate a digital dossier updated continuously throughout the day, covering every activity carried out on the Internet and beyond. Once the target individual has been identified, all these records are lawfully accessible by law enforcement agencies after all relevant safeguards have been put in place. Although some try to refrain from leaving traces on the network, complete anonymity appears impossible to achieve in most developed countries, in which more and more activities are being delegated to the electronic dimension[83].

6.2. *De-emphasizing the "Going Dark" Problem*

At this point of the analysis, it should be inquired whether the problem faced by law enforcement during investigations, because of the difficulties generated by strong encryption, is overemphasized. In paragraph 2, it has been pointed out that the inability to access encrypted communications or devices is the biggest obstacle to investigations. That is because of the given constant and worldwide expansion of default strong encryption in the tech sector, as evidenced by the numbers and statements from stakeholders previously mentioned. How much of this, however, is actually true? In 2016, following the San Bernardino attack, a report from Harvard University's Berkman Center for Internet and Society titled "Don't Panic: Making Progress on the 'Going Dark' Debate" casts serious doubts on these claims, suggesting that the "going dark" issue was overstated[84].

82. Swire and Ahmad, *Encryption and Globalization* at 470 (cited in note 4).

83. See *ibid*.

84. Urs Gasser, et al., *Don't Panic: Making Progress on the "Going Dark" Debate* (Berkman Center for Internet and Society, January 2016), available at https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1 (last visited November 1, 2022).

The basis of the arguments supported by the *Don't Panic* report rested on the fact that, in the first place, this widespread adoption of end-to-end encryption was still far from being achieved. Essentially, because of commercial reasons, it seemed doubtful that it would be achieved even in future. In fact, a cryptographic system that does not allow the service provider access to the contents of the communication collides with the business model of many companies. Indeed, the free or freemium model consists in providing free content to users, which must be financed by personalized advertising revenue. The only way in which targeted advertisements can be offered by obtaining extensive personal data through the behavior and iterations of users on the Internet. Once browsing data are made unidentifiable through end-to-end encryption, the economic sustainability of this mechanism would be wiped out[85].

It should also be considered that cloud computing service providers also widely used today, transmit data and software in a mode of ubiquitous connectivity that allows these data and software to be accessed across multiple platforms. That would be inconceivable in an end-to-end encryption ecosystem as the companies involved need access to plaintext data[86]. Following this trajectory, the result is that end-to-end encryption is unlikely to be the technical standard on which the architecture of the Internet is and will be based.

These operational difficulties, however, do not apply to endpoint encryption, which is increasingly the rule for every device on the market. It is undeniable that unlocking these devices has been made extremely more challenging by this type of encryption. Moreover, on the other hand, the mere fact that end-to-end encryption is not everywhere does not prevent the most cunning criminals from deciding to use only services and products that include it[87]. But this is not a major threat to investigation and surveillance activities. In fact, the advent of the Internet of Things (IoT) has to be taken into consideration. IoT can be defined as a network of physical objects equipped with sensors and processing abilities that allow large-scale, real-time

85. See *id*. at 10-11.

86. See *id*. at 11-12.

87. Manpearl, *Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate* at 79-80 (cited in note 1).

data interchange between them. As in the cases of Smart TVs, Smart Cars, door locks, etc.[88], most of the data transmitted by these "things" are metadata, i.e. data that refer to other data, describing them or giving additional information about them. The peculiarity of metadata is that they tend to be unencrypted. And if we then look at what they can reveal, the benefit that their exploitation might bring to law enforcers' investigations is immediate:

- *Landline telephone*: data on the recipient of the call, at what time and for what duration the call has taken place;
- *Email*: data on the recipient of the mail, at what time, the information on the subject line, and the type of content;
- *Surfing the web*: the device and browser model used, the website visited, page preferences, login details (if auto-fill is enabled), previous interactions with a site (based on authorized cookies), and geographical location;
- *Uploading digital images*: at what time and place photos have been uploaded, with what type of camera, and what settings were set[89].

Pulling the threads together, the complex of metadata outlines overall patterns of an individual's daily life that are inspected using "traffic analysis"[90]. Through this process, law enforcement agencies can intercept and examine encrypted messages by deducing information from patterns in communication[91]. These techniques are very useful, for instance, to break the anonymity of a network, such as TOR[92]. But also to understand the strategies of suspects based on the frequency with which communications are made: deducing the state of activity of a criminal gang and, possibly, the hierarchical relationships between them.

88. See *ibid.*

89. Holly Porteous, *Metadata, National Security and Law Enforcement Agencies* (HillNotes, November 21, 2014), available at https://hillnotes.ca/2014/11/21/metadata-national-security-and-law-enforcement-agencies/ (last visited February 4, 2022).

90. See *ibid.*

91. Ramin Soltani, et al., *Towards Provably Invisible Network Flow Fingerprints*, 51st Asilomar Conference on Signals, Systems, and Computers at 258-262 (2017) available at https://doi.org/10.1109/ACSSC.2017.8335179 (last visited November 1, 2022).

92. See *ibid.*

7. *Conclusions*

The time has come to draw the lines of this essay and weigh up what has been said whereby to identify the desirable direction to take in the present and the future.

The return of encryption to the public discourse has marked a radical polarization between two factions: those who advocate for strong encryption in order to ensure full security in the digital world. On the other hand, the promoters of "crippled" encryption can, if necessary, be bypassed by authorities legitimately dedicated to the pursuit of collective security. In this clash between numerous stakeholders, the needle of the scales is moving frantically without finding common ground.

However, given the intrinsic architectural insecurity of the Internet, it can be argued that strong encryption is the main safeguard against the continuous threats faced in the transmission of communications and transactions. Without it, it would be unimaginable to ensure the confidentiality of correspondence, which inevitably compromises freedom of expression. The same applies to the possibility of concluding commercial operations in a network where any credentials could be easy prey for the malicious. The awareness of Internet users that secure interactions can be enabled has been the basis of its global expansion. Cryptography has evolved into an actual science, refining itself over time, to the point where strong encryption has become a constant in the technology market.

Platforms offering end-to-end encryption prevent anyone but the sender or the receiver from deciphering the content of the communication. Similarly, devices equipped with endpoint encryption prevent unlocking by anyone who does not have the password. Law enforcement and national security agencies thus see their investigative capabilities diminished and are clamoring for tech companies and ISPs to set up a backdoor in their favor to remedy this disadvantage.

Unfortunately, in the current state of the matter, this is not possible without compromising the overall security of the system, even following the most advanced techniques such as those discussed in paragraph 4.

In a seemingly deadlocked situation where a compromise does not appear to be attainable, the choice must fall on the side which prevails

on the basis of a cost-benefit analysis of the fundamental rights here involved. Having clear in mind that encryption technology - and the way it is regulated - merely represents the medium through which this balance should be achieved.

Following the setting line of this essay (and of its title), the clash between strong and weak encryption becomes the bearer of (seemingly) conflicting instances. On the one hand, the protection of national security. Oppositely, the concept of security - in a more generic sense - of the Internet infrastructure as well as of the data of those who, in any way, come into contact with all the economic and personal repercussions that this entails. Within this paradox generated by the use of this technology, it is necessary to observe the bigger picture, so as to succeed in balancing the rights at stake without sacrificing the essential core of any of them.

The bottom line is that without strong encryption, there can be no secure and fully constitutional Internet, according to the requirements set forth by democratic societies. These societies aim to ensure freedom of expression and information, protection of personal data, and a flourishing as well as competitive digital market. At the same time, a provision of legal access to encrypted contents by law enforcement is not necessary to its full extent. This is because the disadvantages of going partially dark are largely offset by the extraordinary surveillance capabilities that the government has at its disposal in a redesigned online society.

Location tracking contacts information and, more generally, the boom of metadata production with the rise of IoT has enabled to build deeply detailed digital dossiers on each individual and their digital interaction. Within this framework, the much-coveted national security is thus saved. Clearly, it is not intended to deny that in some investigations the content of some encrypted communication may be essential to ascertain specific facts and that the lack of an access door may preclude an important investigative contribution or may hinder a preventive strategy. However, what has been argued and constitutes the point of arrival of this essay, is that there are other paths that can be taken to reach the same solution and, in doing so, to be able at the same time to effectively protect digital human rights by ensuring a secure Internet architecture.