Michigan Technology Law Review

Article 5

2020

Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate

Carlos Liguori
Yale Law School

EXPLORING LAWFUL HACKING AS A POSSIBLE ANSWER TO THE "GOING DARK" DEBATE

*Carlos Liguori**

The debate on government access to encrypted data, popularly known as the "going dark" debate, has intensified over the years. On the one hand, law enforcement authorities have been pushing for mandatory exceptional access mechanisms on encryption systems in order to enable criminal investigations of both data in transit and at rest. On the other hand, both technical and industry experts argue that this solution compromises the security of encrypted systems and, thus, the privacy of their users. Some claim that other means of investigation could provide the information authorities seek without weakening encryption, with lawful hacking being one of the most suggested alternatives. "Lawful hacking," also known as "government hacking," consists in the deployment, by investigative authorities, of tools that allow for the intrusion into computer systems, enabling access to its contents. Although this form of investigation seems to be essential in an increasingly connected society, it is important to understand security and privacy risks of different lawful hacking regulatory approaches. Considering that some countries are already enacting legal frameworks related to it, I aim to highlight the issues that should be properly addressed in order to position lawful hacking as one of the viable answers to the "going dark" debate.

* Resident Fellow of the Information Society Project at Yale Law School. Ph.D candidate at the University of São Paulo, Faculty of Law. I would like to thank the Yale ISP community, especially Professor Jack Balkin, Nikolas Guggenberger, Maren Woebbeking, Rafael Nunes, Przemyslaw Palka, Chinmayi Arun, Michael Karanicolas, Jisu Kim, Sari Mazzurco and all the other participants in the ISP Writer's Workshop; the participants of the 2019 Student Symposium on Cybersecurity Policy at Tufts University, especially Professors Susan Landau, Steven Bellovin and David O'Brien; and the CEPI-FGV researchers Guilherme Kenzo dos Santos, João Pedro Favaretto Salvador and Tatiane Guimarães for their invaluable help in the drafting of this note. The views in this note are entirely my own.

TABLE OF CONTENTS

INTRODUCTION

In recent years, the debate on government access to encrypted data in the context of criminal investigations, popularly known as the "going dark" debate, has certainly intensified. On the one hand, law enforcement agencies around the world are pressing for legal rules that restrict the use of strong encryption systems, arguing that its widespread adoption prevents access to data that may be essential to aid criminal investigations. This pressure intensified after popular online services and operating systems began encrypting user data by default—which means that even criminals with no technical knowledge can benefit from the technology and leave law enforcement authorities "in the dark." The solution, they argue, resides in mandatory im-

plementation of exceptional access mechanisms in those encrypted systems, which would enable access to plaintext by authorities.[1]

On the other hand, industry and technical experts contend that the insertion of these mechanisms will weaken the systems in their totality, compromising the security—and, consequently, the privacy—of all their users. In addition, experts point to various issues that could arise from this kind of approach. These issues include (but are not limited to): (i) the limiting of civil liberties and rights that are enabled by the use of strong encryption; (ii) jurisdictional problems from imposing restrictions to services offered internationally; and (iii) the hampering of technological development, as security is increasingly seen as a product differentiator.[2]

Often, alternative means of investigation are suggested in order to steer authorities away from restricting encryption. One of the most suggested alternatives is to focus on "lawful" or "government hacking." This consists of law enforcement authorities deploying hacking tools, such as exploitation of system vulnerabilities or development of malware, in order to access either encrypted data at rest (data that is stored in a device) or in transit (data that is flowing from one device to another through a network). Though specific information is scarce, government hacking has been deployed in practice since at least the 1990s,[3] but its regulation (or lack thereof) has been a subject of debate only recently.

While this form of investigation seems to be essential in an increasingly connected society, it is important to understand possible security and privacy risks of different government hacking regulatory approaches.

Within the context of the encryption debate, several countries are already discussing and implementing laws related to lawful hacking. Some of them sought to regulate the activity *in addition* to the legal regulation of cryptography, such as France[4] and Australia,[5] while others have chosen not

---

1. In the public debate, "exceptional access mechanisms" on encrypted systems are often referred to as "backdoors." "Backdoor [is] a general term describing a mechanism or access point in a communications device or network that enables "the creator of software or hardware [to] access data without the permission or knowledge of the user," Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599, 609 (2016).

2. *See generally* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69 (2015).

3. For an illustrative study on high profile cases of lawful hacking in the United States, see SAYAKO QUINLAN & ANDI WILSON, NEW AMERICA OPEN KNOWLEDGE INSTITUTE, A BRIEF HISTORY OF LAW ENFORCEMENT HACKING IN THE UNITED STATES (2016).

4. *See generally* Bhairav Acharya et al., NEW AMERICA OPEN KNOWLEDGE INSTITUTE, DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: FRANCE (2017).

5. In Australia, government access to encrypted data is regulated by the Telecommunications (Interception and Access) Act of 1997, the Surveillance Devices Act of 2004, and

to regulate encryption. The latter group instead concentrates its efforts on alternative means of investigation, especially lawful hacking, while choosing to leave encryption alone. This group includes countries such as Germany[6] and the Netherlands.[7]

My general perception is that while policymakers are moving forward with legislation related to both government access to encrypted data and lawful hacking, some stakeholders in the public debate seem almost entirely concentrated on denouncing the security and privacy risks of limiting encryption. This group sometimes suggests alternative solutions, but they are not usually explored in depth. I argue that lawful hacking should take the center stage of the "going dark" debate for two reasons: first, it seems to be a better (although imperfect) alternative solution to exceptional access; second, law enforcement agencies already deploy hacking tools for investigative purposes, yet lawmakers are not properly addressing the plethora of issues that come with it.

With this scenario in mind, Part I of this Note briefly describes the background of the "going dark" debate by pointing out the main questions behind it and responses to it. This part will also explore frequently suggested alternatives to mandatory access, with special emphasis on lawful hacking.

Part II aims to identify the main issues that should be considered in the elaboration of a legal framework for lawful hacking by law enforcement. This includes its concept and scope, costs and development, accountability, and jurisdictional problems.

Finally, Part III aims to understand how (and if) those issues are being addressed in recently enacted lawful hacking regulations.

I. THE CONTEMPORARY "GOING DARK" DEBATE

The contemporary debate on encryption regulation and government access to encrypted data has its roots in the late 1990s, shortly after the launch of commercial Internet. Back then, its use was still reasonably restricted to the technical and academic communities, as well as to those able to afford personal computers and an Internet connection. The operating mechanism of the Internet is the same today as it was then: a set of decentralized and transnational networks that connect devices to each other, enabling ex-

---

the Crimes Act of 1914. All those Laws were recently amended by the 2018 Telecommunications and Other Legislation Amendment (Assistance and Access), which reasonably expanded the government's lawful investigatory powers. *See infra* section III.C.

6. *See generally* BHAIRAV ACHARYA ET AL., NEW AMERICA OPEN KNOWLEDGE INSTITUTE, DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: GERMANY (2017).

7. *See* Janene Pieters, *Dutch Parliament Approves Bill to Hack Criminal Suspects*, NL TIMES (Dec. 21, 2016), https://nltimes.nl/2016/12/21/dutch-parliament-approves-bill-hack-criminal-suspects.

changes of information between them.[8] This design makes it simultaneously hard to regulate and structurally insecure.

Cryptographic systems are paramount to overcoming the insecurity of information exchange. They are an integral part of the proper functioning of the Internet since they allow for safe traffic of data between parties and also authenticate the identity of those involved in these operations. Without such systems, banking transactions, communication, and online shopping would be far more susceptible to intrusion and fraud, and therefore less attractive to users. In addition, encryption can also be deployed to protect data stored in computers.

In the mid-90s, U.S. law enforcement and national security agencies[9] began to worry about the prospect of wide adoption of encryption technologies for online communication. They argued that encryption would hinder criminal investigations, particularly law enforcement activity involving the interception of data in transit and access to data at rest in encrypted disks. At the time, a solution provided by the U.S. government was the implementation of a mechanism, developed and provided by the authorities, that would encrypt the data and, at the same time, provide the authorities with the decryption keys through an escrow system. This mechanism was called the *Clipper Chip*—a computer chip that was intended to be acquired by manufacturers and installed on machines marketed in the United States.[10]

The initiative was widely criticized, especially by technical and industry experts.[11] The criticism focused on the fact that cryptographic systems endowed with this type of exceptional access given to third parties would be inherently unsafe in their entirety. It would suffice to foreclose the idea, they argued, that the keys accessible to government agents would fall into the wrong hands and then anyone—including those with less noble intentions than law enforcement—could access private users' data.[12]

In 1994, then-AT&T Bell Laboratories cryptographer Matt Blaze found a vulnerability in the *Clipper Chip* system that allowed for the encryption of data using the system's algorithm (Skipjack) without delivering the key in escrow to the government authority, thus rendering the entire system useless

---

8. P. W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 21-25 (Oxford University. Press 2014).

9. This article aims to focus exclusively on the law enforcement side of the "going dark" debate. For a more in depth look at the national security side and its ramifications, see WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE 77-108 (2007); NAT'L ACADS. SCIS., ENGINEERING, & MED., DECRYPTING THE ENCRYPTION DEBATE: A FRAMEWORK FOR DECISION MAKERS 36-48 (2018).

10. *See* Parker Higgins, *On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures*, ELEC. FRONTIER FOUND. (Apr. 16, 2015), https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures.

11. *See* Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (1997), https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W.

12. *See* Abelson et al., *supra* note 2, at 1.

for its main objectives. This, along with the failure of the *Chip* to be adopted by the market, resulted in the initiative being entirely dropped by the U.S. government in 1996.[13]

There was a shift toward the liberalization of encryption both in the United States and abroad in the early 2000s.[14] Anticlimactically, strong encryption was not immediately adopted by the majority of Internet users and services, who in those early years seemed to be more concerned with ease of use and cost than data security.[15]

Between the *Clipper Chip* initiative and the more recent "going dark" debate, more than a decade passed without encryption being in the spotlight as an issue to law enforcement. In the meantime, the Internet became indispensable to everyone. No longer exclusive to technicians, academics and the wealthiest, the Internet became the main form of communication in society across economic, social, and cultural spheres. Increased use of the network meant greater flow of data and information. Consequently, there was greater reliance on access to this information by criminal investigators. It is in this scenario that the contemporary debate on regulation of cryptography arises.

A. *Framing the Debate: Encryption "By Default" and Mandatory Exceptional Access*

In 2013, Edward Snowden released documents that exposed a complex global surveillance scheme conducted by the U.S. government. The former CIA employee and NSA contractor provided thousands of official documents supporting the allegations.[16] The revelations showed surveillance programs aimed at U.S. and non-U.S. citizens, including governmental authorities from various countries (*e.g.*, former Brazilian President Dilma Rousseff). To enable this scheme, the National Security Agency ("NSA") developed and purchased sophisticated mechanisms for exploiting system vulnerabilities and for data collection. The Agency also accessed and monitored user data pertaining to large companies such as Google, Microsoft, Facebook, and Apple.

---

13. *See* Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, 2 ACM CONF. ON COMPUTER & COMM. SECURITY 59 (1994).

14. Peter Swire & Kenesa Ahmad, *Encryption and Globalization*. 23 COLUM. SCI. & TECH. L. REV. 440 (2012).

15. SUSAN LANDAU, SURVEILLANCE OR SECURITY? THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGY 47 (2011) ("The public, while in principle wanting private communications, in practice appears willing to make it private only if the system is simple to use, does not affect the communications by slowing them down or degrading quality, and cheap (as in little or no cost to the user).").

16. *See generally* Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded, What the Revelations Mean for You*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

The revelations struck the international community, and the issues of privacy and online data protection took the spotlight again. Although the NSA held the majority of the responsibility, much of the negative repercussions also fell on technology companies. Consumers began to distrust the quality and security of their products and services. What followed was the so-called "Snowden effect," in which technology companies addressed privacy and security concerns related to their services in order to regain consumer trust.[17]

In this context, several companies have implemented strong, standardized cryptographic systems in their services . This means that the use of encryption in conjunction with the normal functionality of the application (for example, a messaging app) does not require any type of user opt-in, activation, manual installation, nor any kind of in-depth technical knowledge of encryption techniques. Many popular services have adopted this "encryption by default" approach, including instant messaging applications (WhatsApp, iMessage, and Signal use end-to-end encryption for communications data[18]) and operating systems (such as Apple's iOS, for stored data[19]).

If in the past strong encryption was used only by the few with technical knowledge or those who were required to encrypt by virtue of their professions (such as some lawyers), it is now accessible to even the most casual technology user. Although this has meant more security for general users, the protection and ease of use also applies to non-tech-savvy criminals.

The 2015 San Bernardino terrorist attack was a paradigmatic event for the debate on legal regulation of cryptography and government access to encrypted data. In the attack, sixteen people were killed, including the assailants. During the course of its investigation, the Federal Bureau of Investigation ("FBI") was unable to access the iPhone 5C data of one of the perpetrators.[20]

The phone was updated to Apple's iOS 9 operating system, which meant that access was password protected and its content was encrypted given that iPhone encryption is provided by default. Furthermore, the cell

17. *See, e. g.*, Laura Hautala, *The Snowden Effect: Privacy is Good for Business*, CNET (June 3, 2016), https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection.

18. *See Security and Privacy: End-to-End Encryption*, WHATSAPP, https://faq.whatsapp.com/en/general/28030015 (last visited Mar. 22, 2020); *Technical Information*, SIGNAL, https://signal.org/docs/ (last visited Mar. 22, 2020).

19. *See* Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot*, ARS TECHNICA. (Sept. 18, 2014), www.arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot.

20. It is interesting to note that if the perpetrator's iPhone was a newer model (iPhone 5S onwards), unlocking the contents could be far easier if fingerprint or facial recognition was activated. The iPhone 5C was the last model that did not support these kinds of authentication.

phone also had a second layer of protection against brute force attacks:[21] After ten wrong attempts in the password field, all of the content in the device would be erased.

One outcome of the San Bernardino case was that the FBI asked Apple to develop an operating system that enabled law enforcement to access users' data. Apple resisted the request, claiming that the insertion of the mechanism would weaken the security of its handsets and compromise the privacy of its users.

Faced with the company's refusal, the FBI took Apple to court but then withdrew the complaint in March 2016 after obtaining the requested data with the help of an undisclosed third party. Still, law enforcement authorities have come to denounce the difficulties of strong encryption in the context of criminal investigations, rekindling a fervent international debate over the limits of government access to encrypted data. This is what became known as the "going dark" debate, a term coined by the FBI's former General Counsel Valerie Caproni in 2011,[22] popularized by former FBI Director James Comey in 2014[23] and recently reinforced by current FBI Director Christopher Wray[24] and U.S. Attorney General William Barr.[25]

Far from limiting itself to the United States, the "going dark" debate spread worldwide, and a number of governments have either expressed the need for or passed legislation regarding government access to encrypted data.[26] Mandatory exceptional access is often brought up by government au-

---

21. "Brute force attacks" to encrypted systems refer to trying every kind of possible combination of passwords or pin in the hopes of finding the right one.

22. Valerie Caproni, *Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security*, Washington, D.C. (Feb. 17, 2011), https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

23. James B. Comey, Dir., Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Brookings Institution (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

24. *See* Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html.

25. William P. Barr, Att'y Gen., Keynote Address at the International Conference on Cyber Security, New York (July 23, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

26. According to research conducted by the Centro de Ensino e Pesquisa em Inovação at Fundação Getulio Vargas, between 2010 and 2017, at least twenty-four countries have either officially been discussing or actively implementing legislation that aims to address the issues at stake in the "going dark" debate. Different countries proposed different regulatory approaches to encryption: some are actively stimulating the adoption of strong encryption (Netherlands); some aim to restrict it either by prohibiting its deployment (Iran) or by limiting the size of cryptographic keys (India); other countries require parties (users, vendors, etc.) to provide assistance to law enforcement in accessing encrypted data (Ireland, Mexico). Most of these legal frameworks were enacted fairly recently, and the full extent of their practical ap-

thorities around the globe, such as in Australia, the United Kingdom,[27] and France.[28] While not explicitly requiring companies to alter their systems in order to provide law enforcement access to data, recently enacted laws came under fire for their restrictive approach towards encryption.[29]

B. *Suggesting Alternatives: Enabling Criminal Investigations Without Compromising Encryption*

As law enforcement and other government actors pushed for a regulatory approach that could restrict the use of encryption, a large number of researchers, technical and industry experts, non-profit organizations ("NPOs"), and other actors weighed in against it.[30] They point out that the insertion of these mechanisms will necessarily weaken the systems as a whole, compromising the security of all users—including those not under investigation and those that live outside the jurisdiction in which the policy would be implemented.

As a consequence, they argue, mandatory weakening of encryption can be extremely harmful to the exercise of fundamental rights and civil liber-

---

plicability and effectiveness remain to be understood when applied in specific cases. For a comprehensive analysis and mapping of the debate, see *Cryptomap*, CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO, FGV DIREITO SP (2018), http://www.fgv.br/direitosp/cryptomap.

27. *See* Julia Carrie Wong, *US, UK and Australia Urge Facebook to Create Backdoor Access to Encrypted Messages*, GUARDIAN (Oct. 3, 2019), https://www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption.

28. *See* Sébastian Seibt, *French Candidate Macron Targets Encryption in Fight Against Terrorism*, FRANCE 24 (Apr. 12, 2017). https://www.france24.com/en/20170412-candidate-macron-encryption-fight-terror-whatsapp-telegram.

29. *See, e. g.*, Alex Hern, *UK Government Can Force Encryption Removal, but Fears Losing, Experts Say*, GUARDIAN (Mar. 29, 2017), https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act (implications of the United Kingdom's Investigatory Powers Act of 2016); Lily Newman, *Australia's Encryption-Busting Law Could Impact Global Privacy*, WIRED (Dec. 7, 2018), https://www.wired.com/story/australia-encryption-law-global-impact (implications of Australia's Assistance and Access Act of 2018).

30. *See, e.g.*, DANIEL CASTRO & ALAN MCQUINN. INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, UNLOCKING ENCRYPTION: INFORMATION SECURITY AND THE RULE OF LAW (2016); LEX GILL, TAMIR ISRAEL & CHRISTOPHER PARSONS, CITIZEN LAB AND THE SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC, SHINING A LIGHT ON THE ENCRYPTION DEBATE: A CANADIAN FIELD GUIDE (2018); BERKMAN KLEIN CTR., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK DEBATE" (2016); EASTWEST INST., ENCRYPTION POLICY IN DEMOCRATIC REGIMES: FINDING CONVERGENT PATHS AND BALANCED SOLUTIONS (2018); NAT'L ACADS. SCIS., ENGINEERING, & MED., *supra* note 9; Abelson et al., *supra* note 11; Amnesty Int'l, *Encryption: A Matter of Human Rights*, AI INDEX POL 40/3682/2016 (March 2016); Charles Duan et al., *Policy Approaches to the Encryption Debate*, R STREET POL'Y STUDY 133 (2018); Wolfgang Schulz & Joris van Hoboken, *Human Rights and Encryption* (UNESCO Series on Internet Freedom 2016); Stefan Soesanto. *No Middle Ground: Moving on From the Crypto Wars*, EUR. COUNCIL ON FOREIGN REL. ECFR/263 (2018).'

ties in the digital sphere, especially the right to privacy.[31] These rights are best protected by ensuring the confidentiality and integrity of information shared via the Internet and stored in computer devices. The right to freedom of expression[32] in particular is promoted by enabling communication between parties without fear of surveillance. Reinforcing this position, the Office of the United Nations High Commissioner for Human Rights ("OHCHR") has developed a number of documents highlighting not only the importance of cryptography in this scenario but also the need for States to ensure that the development of the mechanism is promoted and not limited in its use.[33]

To help solve the "going dark" problem, some scholars claim that technological development and the widespread use of data gathering and data generating technologies could represent a plethora of alternatives to law enforcement without compromising encrypted systems. The most prevalent examples of those alternatives are: (i) access to communications metadata; (ii) access to non-encrypted data stored in cloud services; (iii) metadata of Internet of Things ("IoT") devices; and, often cited as a last resort solution, (iv) government hacking. Some scholars suggest that these alternative sources of information and investigation have the potential to enhance law enforcement capabilities so much that we could be living in a "golden age of surveillance."[34]

(i) *Communications metadata* refers to information about communications data, separate from the communication content itself. This category of information may include: device location data, IP address of the sender and receiver of the communications, telephone calling records, and more. This kind of data is often not encrypted—it has to be so in order for telecommunications systems to function[35]—and may provide crucial information for law enforcement agencies without the need to access encrypted data.[36]

---

31. *See* Amnesty Int'l, *supra* note 30, at 10.

32. *See* Schulz & van Hoboken, *supra* note 30, at 51.

33. More specifically, the OHCHR has produced two reports and an international public consultation on the regulation of cryptography. *See* David Kaye, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Human Rights Council on Its Thirty-Second Session, *Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, U.N. Doc. A/HRC/32/38 (May 11, 2016); Frank La Rue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Human Rights Council on Its Twenty-Third Session, *Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).

34. *See* Swire & Ahmad, *supra note* 14, at 464.

35. *See* Berkman Klein Ctr., *supra* note 30, at 3.

36. In Brazil, for example, the use of metadata by law enforcement authorities was paramount in the investigation of two of the most high-profile crimes in recent Brazilian history: the 2011 murder of Judge Patricia Acioli and the 2018 murder of City Counselor Marielle Franco and driver Anderson Gomes. Cellphone location data and browser history—along with

(ii) *Cloud storage* is a kind of online service that has increased in popularity over the past years. For the most part, they consist of premium or freemium[37] services that allow users to store files in remote servers. Those servers, and thus the user's files, can be accessed through any device with an Internet connection.

More often than not, these services are offered by companies that develop operating systems for computational devices: Apple offers iCloud; Google offers Google Drive; Microsoft offers OneDrive. It is pretty common and convenient for users to enable these services when setting their devices. As a consequence, all files generated, received, or sent to devices are replicated and stored in the cloud. Most cloud services store data in a way that allows for the service provider to access it,[38] which means there should be no technical impediment for law enforcement to lawfully require access to a client's data.

The security of cloud services is extremely relevant and widely debated in contemporary data protection studies,[39] and encrypted cloud services seem to be on the rise.[40] However, it seems that non-encrypted cloud services could be an efficient short-term alternative for criminal investigations that does not require compromising cryptographic systems as a whole.

(iii) Another alternative source of information that could aid law enforcement immensely is the *data and metadata provided by Internet of Things ("IoT") devices*.[41] The growing popularity of IoT devices—

---

hundreds of other gigabytes of metadata—were used to find the culprits in both cases. *See* Cecília Ritto*, Inquérito conclui que policiais mataram juíza para evitar pedido de prisão.* VEJA (Sept. 12, 2011*),* https://veja.abril.com.br/brasil/inquerito-conclui-que-policiais-mataram-juiza-para-evitar-pedido-de-prisao/; Márcio Padrão, *Caso Marielle: como celulares levaram a acusados e por que isso é um avanço.* UOL (Mar. 13, 2019), https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/03/13/como-os-celulares-ajudaram-a-achar-o-assassino-de-marielle-franco.htm.

37. Normally, those services offer free storage up to a limited size. After the limit is reached, the user can opt to subscribe to the service in order to acquire more storage space. Google Drive, for example, offers 15GB of storage to users for free, and up to 2TB for paid plans. *See*: GOOGLE ONE, https://one.google.com/about (last visited Mar. 10, 2020).

38. *See* NAT'L ACADS. SCIS., ENGINEERING, & MED., *supra* note 9, at 5, 55. It is important to note that the vast majority of cloud services do use encryption to secure the communication layer between the user and the server where the files are stored.

39. *See, e. g.*, Samuel Lustgarten, *Emerging Ethical Threats to Client Privacy in Cloud Communication and Data Storage*, 46. PROF'L PSYCHOL.: RES. & PRAC. 154 (2015) (for ethics and data protection); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359 (2010); Charles Wharton & K. I. Lin, *Comparative Legislation, Corporate Policy, and Citizen Concerns: Legal Solutions for Privacy Protection in Cloud Computing*, 49 INT'L CARNAHAN CONF. ON SECURITY TECH. 19 (2015) (for comparative regulation)'.

40. *See* Steve O'Hear, *Cloud Storage Startup Tresorit Raises $3M to Put Security Spotlight on Dropbox, Box and Others*, TECHCRUNCH (May 1, 2014), https://techcrunch.com/2014/05/01/tresorit (discussing the European startup Tresorit).

41. *See* Berkman Klein Ctr., *supra* note 30.

networked sensors and devices, such as Smart TVs and Internet-connected GPS—could be a rich source of information for authorities during investigations. Data and metadata from IoT devices tend not to be encrypted and, moreover, those devices often struggle with security issues related to wireless connectivity, outdated software, and hard-to-patch vulnerabilities. Despite those alarming issues in regard to user privacy and data protection, they could nonetheless help authorities access relevant information.

(iv) Finally, the most discussed[42] alternative to overcoming the "going dark" debate is *lawful hacking (or government hacking)*. As previously mentioned in regard to the *Apple v. FBI* case, the FBI withdrew the complaint because it was able to access the encrypted data through a tool purchased from a private company specialized in hacking software.[43] There was, in this case, no mandatory change in Apple's encryption system—the U.S. government used that third-party tool to successfully hack the encrypted device.

Lawful hacking seems to be a viable alternative to the restriction of encryption or the mandatory exceptional access: Instead of requesting technology companies to sabotage their own security systems and knowingly compromise the security and privacy of their users, this alternative focus on observing and exploiting preexisting (and often unintended) security holes. As stated by professors Bellovin, Blaze, Clark and Landau:

> Put simply, the choice is between formalizing (and thereby constraining) the ability of law enforcement to occasionally use existing security vulnerabilities—something the FBI and other law enforcement agencies already do when necessary without much public or legal scrutiny—or living with those vulnerabilities and intentionally and systematically creating a set of predictable new vul-

---

42. *See, e.g.*, EASTWEST INST. *supra* note 30; JAMES A. LEWIS ET AL., CTR. FOR STRATEGIC & INT'L STUDS., THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA (2017); Bert-Jaap Koops & Eleni Kosta, *Looking for Some Light Through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities Against "Going Dark,"* 38 COMPUTER L. & SECURITY REV. 890 (2018); Castro & McQuinn, *supra* note 30; Susan Hennessey, *Lawful Hacking and the Case for a Strategic Approach to "Going Dark,"* in BROOKINGS BIG IDEAS FOR AMERICA 241, 242 (2016); Alan Rozenshtein. *Wicked Crypto*, 9 U.C. IRVINE L. REV. 118, 119 (2019); 'Hoaithi Y. Nguyen, *Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem* (Mar. 2017) (unpublished M.A. thesis, Naval Postgraduate School Monterey) (on file with the Naval Postgraduate School Monterey library system); s*ee also* Sven Herpig, *Government Hacking: Global Challenges*, STIFTUNG NEUE VERANTWORTUNG (Jan. 2018), https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf; Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 590 (2018); Amie Stepanovich, *A Human Rights Response to Government Hacking* (Sept. 2016), https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.

43. *See* Alina Selyukh, *The FBI Has Successfully Unlocked the iPhone Without Apple's Help*, NPR (Mar. 28, 2016), https://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help.

> nerabilities that despite best efforts will be exploitable by everyone.[44]

Even though it is the most suggested alternative to restricting encryption, a proper legal regulation of lawful hacking comes with a complex set of issues that have to be addressed in order to guarantee it is being deployed in accordance with due process and the fundamental rights of investigated parties. These problems will be addressed in the next section.

II. LAWFUL HACKING AS AN INVESTIGATIVE TOOL: REGULATORY CHALLENGES

In a world that is increasingly connected, online, and dependent on data, it makes sense that law enforcement and investigation authorities seek to adapt their activities to this new reality. Digital evidence and cybernetic investigation are fundamental pillars in this scenario. In this sense, lawful hacking seems to be essential in cybercrime cases of great complexity, especially those related to crimes in the darknet[45] (e.g., Operation Onymous, a cooperation between investigative authorities in different countries to overthrow and apprehend responsible parties for illicit markets in the deep web, such as Silk Road 2.0 and Black Market).[46]

In comparison to the mandatory exceptional access approach, lawful hacking presents a better way forward. As stated by Susan Hennessey:

> Instead of creating additional vulnerabilities to an already-fragile security ecosystem in the form of exceptional access, these commentators argued that law enforcement should exploit existing vulnerabilities in software and hardware. In theory, the position offers a workable middle ground by which law enforcement is able to ac-

---

44. Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 5 (2014).

45. For more information on the usefulness of hacking tools to operations on the darknet/deep web, see Orin S. Kerr & Sean D. Murphy. *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law*. 58 STAN. L. REV. 70 (2017).

46. Law enforcement and judicial agencies around the globe undertook a joint action, coordinated by Europol's EC3, the FBI, ICE, HIS and Eurojust, against dark markets running as hidden services on the Tor network. The action aimed to stop the sale, distribution and promotion of illegal and harmful items, which were sold on online dark marketplaces. *Operation Onymous*, EUROPOL, https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous (last visited Mar. 15, 2020). Vulnerabilities in the Tor network (which enables access to much of the deep web content) were used throughout the operation to identify actors and systems used by these websites. *See generally* QUINLAN & WILSON, *supra* note 3.

> cess a sufficient amount of communications and companies are unimpeded in designing secure systems.[47]

However, it is extremely important to highlight the risks posed by lawful hacking in the absence of clear legal and procedural frameworks for its deployment. On the legal side, depending on what is being hacked, the potential for privacy violations can be higher than traditional means of access to information, such as phone wiretapping. On the technical side, there is the issue of informational security weakening: A non-disclosed vulnerability might be discovered by a malicious party and used for its advantage, compromising systems and their users.

There is also the issue of properly disclosing vulnerabilities after their discovery and exploitation. On the one hand, lawful hacking tools can be extremely expensive and hard to find; on the other, the non-disclosure of vulnerabilities used in concluded investigations can directly affect the security and privacy of uninvestigated users of the exploited system and also affect the business model of service providers. Lastly, there is also the fact that lawful hacking can easily transcend national borders and directly affect citizens of other countries.

With that in mind, the next section will further explore the main issues that must be tackled in establishing a legal framework for lawful hacking: (i) legal concept/scope; (ii) prerequisites for deployment; (iii) development and sharing of hacking tools; (iv) accountability and disclosure of vulnerabilities; and (v) jurisdictional issues.

A. *Conceptualizing Lawful Hacking for Legal Purposes*

The first issue in regulating lawful hacking is, naturally, its legal definition. Defining the term and choosing a single expression to reference it seems to be something that is taken for granted in legal scholarship. In reports, papers, and policy briefs it is possible to find "lawful hacking," "government hacking," "law enforcement hacking," and "network investigative techniques" being used to refer to the same general idea of authorities using hacking tools to access data.[48]

---

47. Hennessey, *supra* note 40.

48. For papers using "government hacking," see, e.g., Herpig, *supra* note 42; Mayer, *supra* note 42, at 590; Stepanovich, *supra* note 42. "Law enforcement hacking" is used in QUINLAN & WILSON, *supra* note 2; Mirja Gutheil et al., *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, LIBE COMMITTEE EURO. PARLIAMENT (2017). For "network investigative techniques," see, e.g., Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016) https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques. For this Author's preferred term, "lawful hacking," see generally Bellovin et al., *supra* note 44.

"Lawful hacking" seems to be the most well-suited term, since it is broad with regard to the technical tools and at the same time specific regarding the nature of the activity—it must be expressly permitted by law. "Government" and "law enforcement" hacking do not imply lawfulness nor include the possibility of third parties being involved with the activity (I will further explore this issue in Part II). "Network investigative techniques," in its turn, limits the scope of activity to exploitation of networks—meaning remote access to data—failing to encompass access to seized devices, such as with the San Bernardino iPhone case.

In drafting a legal framework for lawful hacking, one challenge is to conceptualize it without specifically stating the technologies that are used in this approach. Otherwise, technological development will render the framework outdated in no time. Broadly, "hacking" can be defined as:

> the manipulation of software, data, a computer system, network, or other electronic device without the permission of the person or organization responsible for that software application, data, computer system, network, or electronic device, and/or without the permission or knowledge of users of that or other software, data, computers, networks, or devices ultimately affected by the manipulation.[49]

This definition is particularly interesting because it does not limit "hacking" to the exploitation of vulnerabilities in software, firmware, and hardware, and thus the definition also encompasses social engineering techniques (*e.g.*, phishing and water holing). Focusing on hacking's broad objective, gaining access to data, should be the preferred approach.

In this sense, the main applications of lawful hacking can be divided into two main categories: (i) deployment of hacking tools in the context of criminal investigations to remotely access stored or in transit data (*e.g.*, remote installation of malware for surveillance purposes); or (ii) deployment of hacking tools in the context of the forensic examination of a seized hard drive (*e.g.*, breaking into an encrypted smartphone, such as in the San Bernardino case).[50]

Even though both modalities pose obvious threats to privacy and security, the pervasiveness, scope, and risks associated with remote access to data stand out. This distinction should be considered by legislators when determining both the concept and scope of a legal framework for lawful hacking.

B. *Establishing Prerequisites and Limitations*

As is expected with any kind of investigative technique, lawful hacking regulation should be structured in compliance with fundamental rights and

---

49. Stepanovich, *supra* note 42, at 5.
50. *See generally* Mayer, *supra* note 42.

due process in mind. In light of data privacy and system security concerns, a set of *ex ante* considerations must be established in order to limit the use (and, subsequently, the harms) of this approach.[51]

Firstly, this means that legislators must make it explicit that lawful hacking techniques should be employed *ultima ratio*, after less pervasive means of investigation are proven useless to the investigation (even other pervasive means, such as wiretapping). Additionally, in order to avoid abuses, it is imperative to include mechanisms like mandatory judicial authorization for its deployment. A legal framework for lawful hacking should (i) limit the duration of the deployment (relevant to when it is used for monitoring purposes, on the 'remote access to data' category); and (ii) require that law enforcement narrows as much as possible the actors, devices and kinds of information obtained in order for judicial authorization to be granted. A separate challenge regarding judicial authorization is informing and educating judges about the technical aspects of lawful hacking and its possible consequences.

An additional approach could be to allow for the employment of lawful hacking only for the investigation of certain, more serious crimes. Necessity (pondering whether less invasive means of investigation could be used to achieve the same results) and proportionality (weighing the privacy interests of individuals against the government interest as determined by the severity, exigency, and/or perceived threat of the crime) should be considered case by case.[52] In addition to the San Bernardino attack, which was dealt with as a terrorism case, lawful hacking has also been successfully used in high profile investigations on the darknet,[53] specifically regarding crimes of child sexual exploitation (Operation Torpedo[54] (2011) and Operation Pacifier[55] (2015)) and trafficking of drugs and weapons (Operation Onymous[56] (2014) and Operation Bayonet[57] (2017) respectively). This restriction not only prevents abuses but also helps optimize resource allocation, since lawful hacking tools can be rather expensive. This will be further explored next.

---

51. *See generally* Stepanovich *supra note* 42

52. *See generally* Gutheil et al., *supra* note 48.

53. KRISTIN FINKLEA, CONG. RESEARCH SERV., R44827, LAW ENFORCEMENT USING AND DISCLOSING TECHNOLOGY VULNERABILITIES, 2-5 (2017).

54. *Id.* at 3.

55. Dan Alfin, *"Playpen" Creator Sentenced to 30 Years*, FBI NEWS (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years.

56. Andy Greenberg, *Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net* Domains, WIRED (Nov. 7, 2014), https://www.wired.com/2014/11/operation-onymous-dark-web-arrests.

57. Andy Greenberg, *Global Police Spring a Trap on Thousands of Dark Web Users*, WIRED (July 20, 2017), https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap.

C. *Developing and Purchasing Hacking Tools*

Depending on the kind and complexity of the system being accessed by law enforcement, hacking tools can be extremely expensive and hard to come by. This is the case of zero-day vulnerabilities—"a vulnerability discovered and exploited prior to public awareness or disclosure to the vendor."[58] Since popular systems undergo rigorous and constant security checks, zero-days are extremely rare and, upon discovery, quickly patched in system updates. These conditions make hacking tools both expensive and only temporarily useful. The issue that this represents is twofold: Who is going to develop those tools, and who is going to pay for the research and development involved in their elaboration?

With regard to the first question, it is possible to assume three possible alternatives: Authorities can (i) use preexisting public vulnerabilities (such as those found in the National Vulnerability Database[59]), especially when the target is an outdated system; (ii) develop the technology in-house; or (iii) purchase it from a third party—as evidenced in the San Bernardino iPhone case.[60] Purchasing, however, has the potential to incentivize the growth and cultivation of a vulnerabilities market.[61] This could be problematic since these valuable hacking tools could end up in the hands of the highest bidders (which could include anyone from criminals to oppressive governments). The possibility of law enforcement uses skewing the market, however, has been contested by experts.[62] In addition, Bellovin, Blaze, Clark, and Landau[63] argue that third party purchases of hacking tools could also increase incentives against the disclosure of system vulnerabilities.

As for governments developing their own hacking tools, the biggest challenges are costs and complexity. Unlike telephone wiretapping, which often involved a limited number of wiretapping techniques and actors (since

---

58. Bellovin et al., *supra* note 44, at 23.

59. *National Vulnerability Database*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/vuln (last visited Mar. 18, 2020).

60. It has been reported (although not officially confirmed) that the FBI purchased the tool to hack into the locked iPhone for over one million dollars. Danny Yadron, *FBI Admits it Paid $1.3m to Hack into San Bernardino iPhone*, GUARDIAN (Apr. 21, 2016), https://www.theguardian.com/technology/2016/apr/21/fbi-apple-iphone-hack-san-bernardino-price-paid.

61. *See* Riana Pfefferkorn, *Security Risks of Government Hacking*, REPORT - CTR. INTERNET & SOC'Y 5 (2018).

62. "One danger of law enforcement's participation in the zero-day market is the possibility of skewing the market, either by increasing incentives against disclosure of the vulnerability or by increasing the market for vulnerabilities and thus encouraging greater participation in it. Because of the current size of the market and the relatively minimal need by law enforcement, we do not believe that this will be an issue. It is hard to know exactly under which circumstances vulnerabilities will be used since the FBI has not discussed under what technical circumstances they have encountered difficulties wiretapping, but we do believe usage will be rare." Bellovin et al., *supra* note 44, at 47.

63. *Id.*

the tapping is often performed within the infrastructure of the telecom providers), some hacking tools involve meddling with a multiplicity of software, hardware, and security systems. The fact that Lawful hacking solutions tend to be tailor-made for the targeted system adds another layer of difficulty.[64] Moreover, the cost of development is continuous since hacking tools can be rendered useless after the exploited vulnerability is found and patched by the vendor.

This is a common problem in developing countries where investigative authorities are often technologically disadvantaged, and the budget for research and development of investigative tools is not enough to keep up with the rapid pace of information security development.

D. *Disclosing Vulnerabilities*

Though scarce, current scholarly works on lawful hacking seem to agree that one of the most difficult regulatory challenges is the need to report vulnerabilities—either to vendors, targeted individuals or the population in general[65] Scholars seem to agree that the need for disclosure is essential, since existing vulnerabilities might be discovered and exploited by criminals. Nevertheless, only a few scholars have addressed in depth the double-edged sword that the disclosure represents if not properly safeguarded.[66]

On the one hand, it is possible to affirm that lack of proper vulnerability disclosure may generate serious consequences to users after its discovery and exploitation. A recent event that illustrates the possible consequences of government hacking without transparency framework is the WannaCry ransomware. In April 2017, a self-proclaimed hacking group called Shadow Brokers released a series of NSA documents that dealt with cyber weapons developed by the Agency.[67] Several documents dealt specifically with hacking tools, describing vulnerabilities (including a set of zero-days) of popular applications that were exploited to carry out these activities. A widely used vulnerability, dubbed "EternalBlue," was found in the Windows operating system. Although it was patched in later versions, the leaked vulnerability was used to disseminate the WannaCry ransomware, which proliferated in

64. *See* Chen-Yu Li et al., *A Comprehensive Overview of Government Hacking Worldwide*, IEEE ACCESS, 55053, 55065 (2018).

65. *See, e.g.*, Herpig, *supra* note 42, at 20; Li et al., *supra* note 64, at 55066; Rozenshtein, *supra* note 42, at 1208; Stepanovich, *supra* note 42, at 22.

66. On models for evaluating requirements for disclosure, see Bellovin et al., *supra* note 44; Li et al., *supra* note 64; and Stephanie K. Pell & James Finocchiaro, *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid That Process*, 49 CONN. L. REV. 1549 (2017).

67. Lily Hay Newman, *The Leaked NSA Spy Tool that Hacked the World*, WIRED (Mar. 7, 2018, 8:00 AM), https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world.

dozens of countries and affected hospitals, companies, and courts.[68] The same vulnerability was used afterwards to produce another more powerful ransomware, NotPetya, which was even more destructive than its predecessor.[69]

On the other hand, disclosing vulnerabilities may render them useless to law enforcement if the vendor patches the exploit in newer versions of the targeted system.[70] Eventually, if the authorities need to target the system for a subsequent investigation, a new vulnerability must be found and exploited, incurring the costs and efforts mentioned in the previous subsections.

A legal framework for lawful hacking should address at least four important questions regarding vulnerability disclosure:

(i) *Should the vulnerability be disclosed?* The answer to this first and most complex question has to encompass multiple policy and technical considerations. Policy considerations should contemplate all the aforementioned lawful hacking issues; technical considerations should assess the "*significance of the vulnerability's threat to information security"*;[71]

(ii) *When should it be disclosed?* After deciding in favor of the disclosure, a second step is establishing the moment for vulnerability disclosure. Should it happen right after its exploitation for the investigation? Should it occur right after the end of the investigation? Should other factors be taken into consideration?;

(iii) *How should it be disclosed?* Another challenge is developing a way to safely disclose the vulnerability, ensuring that no malicious parties can get ahold of it before the vendor is able to patch the system;

(iv) *To whom should it be disclosed?* It is important to define the parties that are going to be informed of the vulnerability. The vendor of the software/firmware/hardware is the most obvious answer, but other parties could also be affected.

Informing users of the affected system is a particularly sensitive issue. This is important because, depending on what is revealed, criminals could be able to identify the inner workings of the vulnerability and target outdated systems. Efforts to make technology users aware of the importance of software updates for security reasons are mandatory; otherwise, both the

---

68. Brian Barrett*, The Encryption Debate Should End Right Now*, WIRED. (Jun. 30, 2017, 7:00 AM), https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry.

69. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

70. *See* Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303, 314 (2017).

71. Pell & Finocchiaro, *supra* note 66, at 1565–77 (proposing a scoring system based on the Common Vulnerability Scoring System ("CVSS") in order to evaluate the pervasiveness of the vulnerability, its risks, and when to disclose it).

rigorous process of vulnerability disclosure by the authorities and the patching by the vendor could be rendered useless in practice.

E. *Jurisdictional Considerations*

The last issue specifically relates to when lawful hacking is deployed to access data remotely: What if a targeted system or user is located outside of the jurisdiction where the hacking was authorized? The inherent transnational structure of the Internet, along with the ever-growing popularity of cloud services (whose servers are spread around the world) require an enhancement of international treaties regarding law enforcement cooperation for local lawful hacking frameworks to be effective. To understand how these issues are being addressed in actual legal frameworks, the next section will analyze four countries that have recently enacted legislation regarding lawful hacking.

III. COUNTRY-SPECIFIC APPROACHES TO LAWFUL HACKING REGULATION

In response to the "going dark" debate, a number of countries have been both discussing and enacting legislation pertaining to lawful hacking either *in addition to* or *instead of* regulating the development, implementation, and use of encrypted systems. The present section provides an overview of existing lawful hacking-related legislation in Germany, France, and Australia[72] and the uncodified Vulnerabilities Equity Process ("VEP") in the United States. The objective of this section is to understand if the previously listed issues are being addressed in these countries.

Before that, it is important to clarify that this Note does not perform an in-depth analysis of those laws or their application in real cases. There are two main reasons for this. First, most of the legislation was enacted fairly recently; thus, the full extent of its reach has yet to be understood. Second, even if those laws are being enforced on a daily basis, cases that require the employment of lawful hacking techniques tend to be kept secret, at least until the conclusion of the investigation, rendering the casefiles inaccessible.

A. *Germany*

The "going dark" debate in Germany took a very particular approach compared with other countries. Although it was initially reported[73] that

72. The main sources of information for this section, beyond the legislation itself, are the following works: Gutheil et al., *supra* note 48; *Cryptomap*, *supra* note 26; *Government Access to Encrypted Communications*, LAW LIBRARY CONG. (2016).

73. Natasha Lomas, *Encryption Under Fire in Europe as France and Germany Call for Decrypt Law*, TECHCRUNCH (Aug. 24, 2016, 7:40 AM), https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law; *France, Ger-*

Germany was pushing for a restriction of encrypted systems, it opted to refrain from regulating cryptography along the lines of the aforementioned regulatory approaches. Germany instead focused on establishing a more robust legal framework for lawful hacking activities.

Over the past ten years, a more concrete approach to lawful hacking activities has been delineated both through legal norms and case law. This culminated in a reform of the German Code of Criminal Procedure (*Strafprozessordnung*, or "StPO") in August 2017 that addressed those developments.

With regard to case law predating the StPO reform, a 2008 decision of the German Federal Constitutional Court (*Bundesverfassungsgericht,* "BVerfG") is considered a landmark case. It was the first ruling on a law[74] that granted law enforcement authority to "secret[ly] access information technology systems."[75] In the ruling, the court defined that this "secret access" meant "technical infiltration that takes advantage of vulnerabilities of the targeted system, or that is carried out by the installation of a spy program."[76] The decision stated that this kind of "secret access" is inherently unconstitutional except in cases where either the exploitation is merely used to access the content of communications in accordance with preexisting lawful intercept legislation or if there is a "concrete danger to a predominantly important legal interest."[77]

Beyond those judicial developments, there are two main laws that regulate government hacking activities: the Federal Criminal Police Office Act of 1997[78] (*Bundeskriminalamtgesetz*, "BKAG"), an administrative Law that regulates the activity of law enforcement authorities, and the aforementioned German Code of Criminal Procedure.[79]

Paragraph 49[80] of the BKAG explicitly establishes that the Federal Crime Police Office may collect data in the course of investigations through intervention in computer systems. However, the norm restricts the use of the technique to investigations that involve danger to life, limitations to freedom, and national security. The BKAG also restricts the deployment of the

---

many Want Messaging Apps to Limit Encryption to Fight Terrorism, GLOBAL NEWS (Aug. 23, 2016, 9:15 AM), https://globalnews.ca/news/2897557/france-germany-want-messaging-apps-limit-encryption-to-fight-terrorism.

74. More specifically, the Verfassungsschutzgesetz Nordrhein-Westfalen [VSG NRW] ["North-Rhine Westphalia Constitution Protection Act"], Dec. 20, 1994 (Ger.)

75. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Feb. 27, 2008, 1 BvR 370/07 (Ger.).

76. *Id.*

77. *Id.*

78. Bundeskriminalamtgesetz [BKAG] [Federal Criminal Police Office Act], July 7, 1997, BGBL I at 1650, repealed May 25, 2018, BGBL I at 1354 (Ger.).

79. STRAFPROZESSORDNUNG [StPO] [CODE OF CRIMINAL PROCEDURE], July 4, 1987, BGBL. I at 1074, as amended Mar. 3, 2020, BGBL. I at 431 (Ger.).

80. BKAG § 20k.

technique to targets that are either suspects in the case being investigated or are communicating with suspects. There is also a maximum limit of three months for data intercept in this modality.

The StPO, by contrast, is more detailed and encompassing. In regulating lawful interception, hacking is allowed as an "annex competence," meaning that it is permitted to facilitate the interception (such as allowing access to encrypted communication before it is encrypted). In addition, German law enforcement may also use any means necessary to access encrypted data on seized devices—which naturally includes hacking the device.[81] On August 17, 2017, the Act to Make Criminal Proceedings More Effective and Practicable[82] (*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*) was enacted and amended the StPO in order to expand the powers of the German authorities to conduct online searches[83] and source telecommunications surveillance.[84]

The StPO also includes a number of *ex ante* and *ex post* measures for the interception of communication must be met. In regard to *ex ante* considerations,[85] authorization of a court is required. The StPO allows the government to bypass court authorization in urgent cases, but authorization must be confirmed by a court within three days. For approval, an interception must meet the following requirements: (i) there is reasonable suspicion of the investigated individual; (ii) the accessed data will not reach the core of the individual's private life; and (iii) the interception request must specify the data being accessed.

In regard to *ex post* considerations, the authorities are required to inform the target of the hacking as early as possible without prejudice to the investigation itself.[86] In addition, law enforcement authorities must issue annual transparency reports to the Federal Office of Justice containing: (i) the number of procedures in which government hacking was deployed for access to data; (ii) the number of judicial orders; (iii) the means used in the investigation; (iv) the description of the targeted systems and the changes

81. Gutheil et al., *supra* note 48, at 79.

82. Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens [Act to Make Criminal Proceedings More Effective and Practicable], Aug. 23, 2017, BGBL. I at 3206 (Ger.).

83. An online search consists of "obtaining technical access to an information technology system from a suspect without his or her knowledge for the purpose of extracting data." StPO §100b. Before it was purely a case law construction, but the reform created section 100b of StPO, which outlines the requirements for online searches that are not related to lawful interception. *Id.*

84. The source telecommunications surveillance allows the investigating authority to obtain access to source data prior to encryption in the context of a telecommunications interception request. *Id.* § 100a.

85. *Id.* § 100a-g.

86. *Id.* § 101(5).

done to it; (v) the criminal type that led to the procedure; (vi) and information on the data collected.[87]

Paragraph 100a of the StPO establishes that lawful access to data is only allowed in certain cases of serious crimes, with paragraph 100a(2) providing an exhaustive list of those crimes. However, the list has been criticized for being overbroad and general; there are twenty-five subsections in §100a(2), and crimes vary from specific (murder and manslaughter) to subjective (crimes against public order).

B. *France*

France's regulatory responses to the "going dark" debate involved both encryption and government hacking activities. In 2016, the French Code of Criminal Procedure (*Code de Procédure Pénale*,[88] "CPP") was amended by the LOI nº 2016-731 of 2016,[89] aiming to "reinforce the fight against organized crime, terrorism, and its financing" ("*renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*"). The text was altered to include devices that strengthened investigatory powers concerning access to encrypted systems and deployment of hacking techniques.[90]

Before the amendment, the French Criminal Code (*Code pénal*) already criminalized the refusal to deliver the means for decryption of an encrypted content when required by authorities.[91] The amendment hardened the punishment for that crime.[92]

In regard to lawful hacking, the amendment altered and included devices on Chapter II of Title XXV in the CPP that deal with the two main functionalities of the technique. Section 5[93] was altered in order to encompass, alongside traditional lawful means of interception (such as wiretapping), the use of digital tools for its conduction. Section 6bis[94] was included in order to regulate investigatory powers related to access to computer data in the following modalities: (i) remote access initiated by the physical installation of

87. *Id.* § 101b.

88. CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] [CRIMINAL PROCEDURE CODE] (Fr.).

89. Loi 2016-731 du 3 Juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (1) [Law 2016-731 of June 3, 2016 Strengthening the Fight Against Organized Crime, Terrorism and Their Financing, and Improving the Efficiency and the Guarantees of the Criminal Procedure (1)], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANCAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 3, 2016 (Fr.).

90. Gutheil et al., *supra* note 48, 73-76.

91. CODE PÉNAL [C. PÉN.][PENAL CODE] art. 434-15-2 (Fr.).

92. *See* Acharya et al, *supra* note 4, at 4.

93. Code de Procédure Pénale [C. Pr. Pén.][Criminal Procedure Code] art. 706-95 to 706-95-10 (Fr.).

94. *Id.* art. 706-102-1 to 706-102-9.

spyware on targeted computer of the investigation; and (ii) access to computerized data carried out entirely remotely.

The CPP also established a set of *ex ante* and *ex post* requirements that must be considered in relation to lawful hacking. *Ex ante* considerations include: an exhaustive (albeit broad) list of crimes[95] that establish when this means of investigation is allowed, particular procedures for obtaining warrants, and a time limit for the conduction of the investigation.[96] *Ex post* considerations are centered on inspection and supervision of those activities by authorities.[97]

Surprisingly, even though the framework is reasonably thorough, there seems to be no legal device concerning transparency and accountability of lawful hacking activities, vulnerabilities, or impacted individuals.[98]

C. *Australia*

Government hacking regulation in Australia, unlike the other countries discussed above, does not have a specific law pertaining to it. Instead, the regulation is spread across multiple Acts enacted throughout different decades. Similar to France, however, the Australian government enacted legislation that aims to both enhance law enforcement's hacking powers and regulate the use of encrypted systems.

The basis for lawful hacking regulation in Australia can be found in two laws from the 1970s: The Telecommunication (Interception and Access) Act of 1979 ("TIA Act") for law enforcement purposes, and the Australian Security Intelligence Organization Act of 1979 ("ASIO Act") for intelligence purposes. The TIA Act is the main law on government intercept of communications of Australian citizens. It is used to authorize interception because its language is broad enough to encompass modalities beyond telephone wiretapping.[99] The ASIO Act establishes the procedure for Intelligence Authorities to obtain the required warrants for the investigation. Gutheil et al[100] note that Section 25A[101] of this Act can be understood as the first Australian law that deals with legal hacking, in this case specifically by the Australian Secret Service. This is because, despite not mentioning "hacking" specifically, it determines the possibility of authorities targeting "computers . . . systems of computer . . . computer networks; or any combination of the above," which opens up a range of systems for the Australian authorities to target.

---

95. *Id.* art. 706-73, 706-73-1.
96. *Id.* art. 706-102-3.
97. Gutheil et al., *supra* note 48, at 74-75.
98. *Id*. at 75-76.
99. *See Telecommunications (Interception and Access) Act 1979* (Cth) (Austl.).
100. Gutheil et al, *supra* note 48, at 114.
101. *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A (Austl.).

A piece of legislation that deals more directly with the techniques employed in hacking activities can be found in the Surveillance Devices Act of 2004 ("SD Act").[102] Among other things, it regulates the ability of law enforcement authorities to install and use surveillance devices. Surveillance devices are defined in Section 6 as "any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer." This encompasses any electronic device capable of storing or processing information, including cell phones, tablets, laptops, routers, etc.

In order to perform this kind of investigation, a judicial warrant is mandatory along with other requirements. There must be reasonable grounds to suspect that a particular individual uses the exploited service; the information obtained should assist in the investigation of one or more serious offenses in which the investigated person is involved; and all other investigative means must be exhausted so that the warrant for access to telecommunications can be given.[103]

The recently enacted Telecommunications and Other Legislation Amendment (Assistance and Access) Act of 2018[104] amended all previously mentioned laws, addressing both the encryption debate and expanding investigatory powers in regard to access to computer data (both communications and stored information). In late 2018, the law (then still a bill) came under fire for being overwhelmingly vague, possibly allowing for interpretation that could lead to the weakening of encrypted systems.[105]

Lastly, the transparency and accountability of Australian government hacking power and activities is likely to be problematic, since Article 37 of the Freedom of Information Act of 1982[106] gives law enforcement authorities the right to refrain from doing so.[107] This has been the target of criti-

102. *Surveillance Devices Act 2004* (Cth) (Austl.).

103. *Telecommunications (Interception and Access) Act 1979* (Cth) s 46 (Austl.).

104. *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (Austl.).

105. *See, e.g.*, Ariel Bogle, *"Outlandish" Encryption Laws Leave Australian Tech Industry Angry and Confused*, ABC NEWS (Dec. 7, 2018) https://www.abc.net.au/news/science/2018-12-07/encryption-bill-australian-technology-industry-fuming-mad/10589962; Lily Hay Newman, *Australia's Encryption-Busting Law Could Impact Global Privacy*. WIRED (Dec. 8, 2018), https://www.wired.com/story/australia-encryption-law-global-impact; Jamie Tarabay, *Australian Government Passes Contentious Encryption Law*. N.Y. TIMES (Dec. 6, 2018) https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

106. *Freedom of Information Act 1982* (Cth) (Austl.).

107. "(1) A document is an exempt document if its disclosure under this Act would, or could reasonably be expected to . . . (b) disclose, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to the enforcement or administration of the law; (2) . . . (b) disclose lawful methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those

cism,[108] especially because the Australian legal order does not have a robust fundamental/human rights protection law.

D. *United States*

Despite the relatively long history of lawful hacking in the US,[109] the country does not have a specific legal framework for its deployment. There are, however, two regulatory mechanisms of note: (i) Rule 41(b)(6) of the Federal Rules of Criminal Procedure ("FRCP") and (ii) the Vulnerabilities Equities Process.

In 2016, the FRCP was amended in order to extend the powers related to searches of computer devices. Rule 41(b)(6)[110] basically grants judges the power to authorize remote access to computers by federal law enforcement agencies. The amendment expanded *"*the reach of the [FRCP] under two circumstances: when a suspect has hidden a device using technological means, and when the [law enforcement agencies] can identify devices located in multiple jurisdictions. These amendments make it possible for [law enforcement agencies] to obtain judicial warrants to search for computers located in unknown or multiple locations."[111]

Those alterations came under fire because of the lack of safeguard mechanisms, the potential for bulk hackings and jurisdictional problems.[112]

Even more interesting is the Vulnerabilities Equities Process ("VEP"). VEP is an administrative deliberation process conducted by U.S. government authorities to determine whether to disclose or keep zero-day vulnerabilities that are used for law enforcement and intelligence purposes, along with its subsequent process for disclosure.[113] Most of the decision-making process is conducted by the Equities Review Board, an intra-agency deliberation forum.[114]

---

methods or procedures; or (c) prejudice the maintenance or enforcement of lawful methods for the protection of public safety." *Id.* para 37.

108. *See* Gutheil et al, *supra note* 48, 113-14.

109. *See generally* QUINLAN & WILSON, *supra note* 3.

110. "[A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts." FED. R. CRIM. P. 41(b)(6).

111. Li et al., *supra* note 64, at 55061.

112. *See* Steven M. Bellovin, Susan Landau & Matt Blaze, *Insecure Surveillance: Technical Issues with Remote Computer Searches*, 49 IEEE COMPUTER 14, 14 (2016).

113. Pell & Finocchiaro, *supra* note 66, at 1554

114. Composed of the following U.S. government agencies: the Office of Management and Budget; the Office of the Director of National Intelligence; the Department of the Treasury; the Department of State; the Department of Justice (including the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force ("NCIJTF")); the Depart-

Due to its classified nature, information about the VEP has always been scarce. It has been reported that the process has been discussed in some form since at least the late 2000s, but its existence was only confirmed in 2014.[115]

After the EternalBlue and WannaCry/NotPetya situations in 2017, the U.S. government published a more in-depth document on the inner workings of the VEP.[116] The document details the structure and workflow of the Equities Review Board and the VEP Executive Secretariat, the decision-making procedure, and the process for the dissemination of the vulnerability. Moreover, the document also puts forth what is taken into consideration by the Board when evaluating the need for vulnerability disclosure, divided into four main categories: (i) impact on the system and its users; (ii) operational impact and value for law enforcement and intelligence; (iii) commercial impact; and (iv) risks for U.S. international relations. [117]

While the idea and structure of the VEP are commendable, the lack of a legal framework that pushes toward transparency and accountability makes it hard to evaluate the actual effectiveness of what is deliberated by the Board.

---

ment of Homeland Security (including the National Cybersecurity Communications and Integration Center ("NCCIC") and the United States Secret Service ("USSS")); the Department of Energy; the Department of Defense (including the National Security Agency ("NSA") (including Information Assurance and Signals Intelligence elements), the United States Cyber Command, and the Department of Defense ("DoD") Cyber Crime Center ("DC3")); the Department of Commerce; and the Central Intelligence Agency ("CIA"). *Vulnerabilities Equities Policy and Process for the United States Government* at 3 (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20 Unclassified%20VEP%20Charter%20FINAL.PDF.

115. This happened because of a Freedom of Information Act ("FOIA") lawsuit made by the Electronic Frontier Foundation ("EFF") against NSA, regarding the Agency's use of a vulnerability called "Heartbleed." "Complaint for Injunctive Relief for Violation of the Freedom of Info. Act, 5 U.S.C. § 552 at 4-5, Elec. Frontier Found. v. NSA, No. 14-cv-03010, 2016 WL 1059389 (N.D. Cal. Mar. 17, 2016). Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator of the Obama Administration, addressed the VEP in a blog post. Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE: PRESIDENT BARACK OBAMA (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

116. *See Vulnerabilities Equities Policy and Process for the United States Government*, *supra* note 114.

117. *Id.* at 13-14.

CONCLUSION: TAKING LAWFUL HACKING TO THE CENTER STAGE OF THE "GOING DARK" DEBATE

The debate on government access to encrypted data is far from over.[118] Law enforcement agencies around the world continue to push for regulation that restricts the use of encryption, while industry and technical experts keep pointing out security and privacy issues that could ensue from this kind of regulation. In this regard, alternative means of investigation such as metadata, non-encrypted data stored in the cloud and lawful hacking are often suggested. Over the past few years, some countries have been proposing or enacting laws to address this issue, adopting different regulatory approaches. Some of those approaches focus solely on the limitation of encryption technologies while others encompass proposed alternatives, specifically lawful hacking.

The problem is that, although lawful hacking is definitely a more desirable alternative to the restriction of encryption, the debate on *how* lawful hacking should be regulated is still in its early stages. Nevertheless, countries not only already deploy hacking tools for criminal investigations, but also maintain laws aimed towards these tools that are failing to address the multitude of issues posed by lawful hacking.

A robust legal framework for lawful hacking is needed in order to enable law enforcement investigatory activities on the one hand, and safeguard security, fundamental rights, and due process on the other. The hurdles to establishing this framework are what should take center stage in the "going dark" debate. Five of its most complex challenges were highlighted in this Note:

- *Defining "lawful hacking" for legal purposes*: What kind of activities does "lawful hacking" encompass? Also, a distinction between hacking devices on site and accessing devices remotely should be outlined, due to the more intrusive nature of the latter.

- *Establishing prerequisites for deployment*: Lawful hacking regulation must be based on its *ultima ratio* character due to its pervasiveness. Along with that, its deployment should require

118. In October 2019, U.S. Attorney General William Barr, along with officials from Australia and the United Kingdom released an open letter to Facebook, addressing the company's intent to expand encryption by default in its unencrypted messaging services Instagram Direct and Facebook Messenger. The officials urged the company to "enable law enforcement to obtain lawful access to content in a readable and usable format," reinforcing all that was put forth over the last half decade of the "going dark" debate. Letter from Rt. Hon. Priti Patel MP, U.K. Sec'y State Home Dep't, et al., to Mark Zuckerberg, Chief Exec. Officer, Facebook (Oct. 4, 2019), https://assets.documentcloud.org/documents/6450624/US-UK-Australia-letter-to-Zuckerberg-10-4-19.pdf.

judicial authorization and be limited to certain crimes based on their gravity.

- *Developing and purchasing hacking tools*: Special attention should be given to the acquisition of hacking tools from third parties so as to avoid legitimizing the growth and cultivation of a "vulnerabilities market" where those tools could end up in malicious hands.

- *Disclosing vulnerabilities*: Perhaps the biggest challenge of them all is establishing *if* and *how* to disclose vulnerabilities used by law enforcement. The need for accountability and transparency in regard to hacking activities seems to be a point of agreement among scholars, but little is discussed in regard to its operationalization.

- *Jurisdictional issues*: Specifically in regard to the remote access modality, the last challenge is how to address the effect of local lawful hacking activities beyond borders. This is complicated by the inherent transnational nature of the Internet.

Despite these challenges, lawful hacking still stands as a preferable substitute to mandating exceptional access to encrypted systems. It should take center stage in the "going dark" debate, with efforts focusing on how to best develop a legal framework that enables law enforcement activities and respects fundamental rights.

It is a viable approach that must be carefully discussed, analyzed, and regulated in order to avoid a future that is singularly bright for law enforcement and entirely dark for user privacy and security.