The Law of the Trojan Horse

Eldar Haber[*]

The use of malware in criminal investigations might be expanding. While "police hacking" is often publicized as used almost solely against pedophiles on the Dark Web, revelations from Israel on extensive police use of malware for a variety of criminal suspects might suggest that more intrusive forms of police hacking may emerge anywhere. Equipped with a wiretap warrant and malware, Israeli police forces can legally bypass encryption and directly obtain content and metadata from the device and its linked apps, turn on a suspect's camera or microphone, and essentially gain full access to the past and present of suspects. While the scope of police hacking in the U.S. is currently unknown, as this Article further argues, the legal framework that governs "search," access to stored communications and wiretaps could authorize such a practice much like in Israel, although it was never designed to do so. This obsolete framework to properly govern the use of malware by enforcement agencies must be updated and reconfigured.

While reflecting on Frank Easterbrook's famous "law of the horse" argument, this Article suggests that trojan horses (malware) must be directly and individually regulated, especially in the realm of criminal law enforcement. This Article explores the history and legality of police hacking under the current legal framework. It then examines the impact of such practice on human rights, human liberties, and other externalities stemming from its use. It moves to propose a blueprint for policymakers on how to regulate police hacking properly, not before placing an almost absolute moratorium on its use until such regulation occurs. Police hacking should be allowed in some circumstances and under a rigorous, semi-technological

[*] Copyright © 2024 Eldar Haber. Associate Professor, Faculty of Law, University of Haifa; Director, The Haifa Center for Law & Technology (HCLT), Faculty of Law, University of Haifa. I am very grateful to Shir Bochlin and Dor Silman for their research assistance. All mistakes are mine.

oversight regime, as this Article suggests, but more importantly, such policymaking is crucial to draw a clear line for when it cannot be used.

TABLE OF CONTENTS

INTRODUCTION

Malicious software ("malware") might soon become a primary investigative tool that enforcement agents use to locate crime, identify culprits, and gather evidence. Such hypotheses stem, inter alia, from the embedding of computers into the daily routine of most individuals, who surround their lives with digital devices that can capture almost everything. Along with often working with computers or being surrounded by Internet of Things ("IoT") devices, mobile phones, which most individuals carry around everywhere,[1] have become essential multitasking computers for doing almost everything: from shopping to learning, reading, and communicating with others. These individuals include culprits, who are likely to use computers in a somewhat similar manner.

Due to such use, enforcement agencies worldwide have begun to realize that wiretapping traditional telephones, placing microphones ("bugs") within a suspect's surroundings, or searching for physical evidence is too limited, time-consuming, or otherwise inapplicable to capture culprits.[2] In addition, many criminals are "Going Dark,"[3] i.e., transitioning into using more secure and encrypted networks, some even through the so-called "Dark Web" (via Tor or other browsers), making their tracking and identification nearly impossible.[4] Enforcement agents are thus left without effective ways to enforce the law.[5]

To overcome the "Going Dark" problem, law enforcement agencies often use malware that can bypass almost any encryption or access to a

[1] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2218-20 (2018) (noting that individuals "compulsively carry cell phones with them all the time").

[2] *See infra* Part I.A.

[3] For more on the "Going Dark" argument, see *id.*

[4] The Onion Router ("Tor") is an open-source platform that enables anonymous user communication and conceals IP addresses by routing traffic through relays while the transit data is encrypted. See, e.g., KRISTIN FINKLEA, CONG. RSCH. SERV., R44101, DARK WEB 3-4 (2017), https://fas.org/sgp/crs/misc/R44101.pdf [https://perma.cc/W73R-DUJ7] (explaining about the Dark Web); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 576 (2018) ("Usage of the Tor anonymization software, for example, has roughly doubled since fall 2013."); THE TOR PROJECT, https://www.torproject.org (last visited Sept. 21, 2023) [https://perma.cc/S693-KW5T] (the website of Tor).

[5] *See infra* Part I.A.

suspect's device. Equipped with such malware, or, "trojan horses,"[6] police officers often connect to the Dark Web and install them in suspects' computers, often those who engage in child pornography, to identify and capture them.[7] But such trojans can also be used more broadly beyond the Dark Web, granting the police a tool to connect to one's phone, see what the user does in real-time, open their microphone and camera, and potentially extract any data and metadata that is linked to the device.[8] Such actions are commenced remotely without suspicion or action on the user's behalf ("police hacking").[9]

Such police hacking might sound fictional, even authoritarian-like. It is not. The proliferation of hacking tools made such spyware widely used by governments worldwide.[10] And as revealed in Israel by a journalist, in an almost Snowden-like moment, police hacking on an unprecedented scale in a democratic regime has been ongoing for years under an

[6] The term "trojan horse" refers to malware disguised as a harmless file. This terminology is inspired by the tale of the wooden horse used to deceive the guards of Troy and sneak soldiers into the city. Numerous types of trojan viruses that can perform various functions can be found online. The primary goal of most trojans is to gain control of a user's computer, steal their information, and spread additional malware on the victim's system. It will be used interchangeably with malware in this Article. *See What Is a Trojan?*, NORTON (Aug. 8, 2018), https://il.norton.com/blog/malware/what-is-a-trojan [https://perma.cc/S6TV-NCTZ].

[7] *See infra* Part I.A.

[8] *See id.*

[9] *See infra* note 23.

[10] As revealed by an investigative journalism consortium (Forbidden Stories) in July 2021, governments believed to be using NSO Group's software are Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates. *See* Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani & Michael Safi, *Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon*, GUARDIAN (July 18, 2021), https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus [https://perma.cc/W8CJ-44CU]. Overall, at least 65 governments have acquired commercial spyware surveillance tools. *See* Hum. Rts. Council, Annual Rep. of the U.N. High Commissioner for Human Rights and Reps. of the Office of the High Commissioner and the Secretary-General, U.N. Doc. A/HRC/51/17, at 2-3 (2022) [hereinafter U.N. Report].

outdated wiretap law that was never meant to grant such broad access.[11] The Israeli police, as later reaffirmed by a governmental report,[12] systematically used Pegasus, a highly sophisticated and intrusive zero-click malware, against a variety of suspects, sometimes remotely linked to a criminal investigation, under secretive court orders. Once sent to a suspect, Pegasus infiltrates a device's operating system and grants full access to the user's stored and real-time communication.[13]

Police hacking is thus not solely reserved for authoritarian regimes but also democratic ones. While such use by U.S. police might sound implausible, police hacking in the U.S. is highly opaque. Currently, police forces publicly declare that while they have examined the use of spyware equivalent to Pegasus before, they decided to refrain from purchasing it.[14] Available data suggests that police forces in the U.S. only use spyware in minimal instances, almost solely for child pornography and on the Dark Web,[15] and are often limited to identifying and locating suspects.[16] But much like how citizens of Israel discovered the extensive use of such intrusive surveillance tools, similar revelations could occur elsewhere, including in the U.S. And even if U.S. police officers are not currently using malware outside the realm of the Dark Web, they are likely to expand their use of this practice under the current regulatory regime due to the increased use of encrypted technologies. Thus, the legal aspects of such use must be further examined.

This Article further posits that police hacking could represent one of the most significant threats to human rights and liberties in the history of criminal investigations in democratic regimes. If the police can legally search and wiretap one's computer and any device within their vicinity, they can effectively trespass into their digital and physical domains, all under the highly general umbrella of public safety. Regulators must

[11] *See* Tomer Ganon, *Israel Police Uses NSO's Pegasus to Spy on Citizens*, CTECH (Jan. 18, 2022), https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html [https://perma.cc/X647-G2KX].

[12] *See id.*

[13] *See* Kirchgaessner et al., *supra* note 10.

[14] *See infra* Part I.A.

[15] *See infra* note 96.

[16] *See* Ivan Škorvánek, Bert-Jaap Koops, Bryce Clayton Newel & Andrew Roberts, *"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking*, 2019 BYU L. REV. 997, 1029 (2019).

oversee that such abilities are not too intrusive and compliant with the legal framework that governs such use. And while there might already be a legal framework to govern police hacking, perhaps mostly under the protection of the Fourth Amendment and the Electronic Communications Privacy Act,[17] it was never crafted for spyware use. As this Article further argues, unlike Frank Easterbrook's famous "law of the horse" argument,[18] trojan horses must have a specific legal framework that would carefully grant such intrusive powers and delineate its borders, all based upon a proper legal debate on the ways such a framework should be constructed. Policymakers must turn to this discussion today before such police use is normalized, as in Israel and in other countries.

This Article essentially asks a "What if" question. What if tomorrow morning, you wake up to discover that police forces across the U.S. have been using malware for years outside the Dark Web, much like they do in Israel? Is such practice legal under U.S. law, and should it be? Which concerns does it raise? And what should the legal framework that eventually governs this practice look like? This Article thus scrutinizes whether the police should be allowed direct access to a suspect's phone using malware and under which conditions. It shifts attention from the legal landscape that enables wiretapping and searching stored communication to potential real-time intrusive surveillance that the legal regime might enable today.[19] It is further divided into two main parts: Part I explores the road from wiretapping to the official use of "Network Investigative Techniques" ("NITs"), or more simply stated, malware. It then examines the legality of police hacking under the current legal framework that governs it and concludes that at least under its legal regime, the U.S. might experience similar revelations as

[17] *See infra* Part I.B.

[18] In the mid-1990s, Judge Frank Easterbrook sparked an academic debate on the "law of the horse," arguing that cyberspace, like horses, does not deserve its own category within lawmaking. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207 (1996). Since then, much has happened. Technology evolved at an incredible rate, and academics and policymakers worldwide found themselves constantly researching and regulating cyberspace due to these rapid changes and developments. *See, e.g.*, Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (contesting Easterbrook's argument).

[19] *See infra* Part II.

in Israel. Part II turns to evaluate the various human rights and liberties affected by police hacking outside the realm of the Dark Web, along with arguing that it creates many other externalities that must be further examined before it is allowed. The Part then offers a blueprint for policymakers to regulate police hacking for the first time while directly offering policymakers a toolkit for properly addressing its ramifications.

I. FROM WIRETAPPING TO COMPUTER HACKING

Criminal investigations require striking a balance between human rights and public safety. With the rise of available technological tools, police officers often sought ways to use them for investigatory purposes.[20] The balance between such human rights and liberties was not always immediate. In many instances, it took a while until policymakers intervened and regulated the legal playing field of such new technologies and their use by the police.[21]

As this Part further shows, while accessing computers for criminal investigation purposes is hardly a new practice, its applicability to the daily lives of individuals seems almost irrelevant at first hand.[22] Currently, the practice and the analysis of "police hacking," a topic that other scholars have addressed in the past,[23] is almost solely reserved for

[20] *See infra* Part I.A.

[21] *See id.*

[22] *See id.*

[23] Sometimes referred to as "lawful" or "government hacking," among other names. *See, e.g.*, Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014) (discussing lawful hacking); Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1123 (2017) (discussing law enforcement in the Dark Web); Mayer, *supra* note 4 (discussing governmental hacking); Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303 (2017) (discussing the use of malware by law enforcement); Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315 (2015) (discussing the use of malware by law enforcement). For a comparative analysis of police hacking regulation in Germany, Italy, the Netherlands, the United Kingdom, and the U.S., see Carlos Liguori, *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*, 26 MICH. TELECOMM. & TECH. L. REV. 317, 336-43 (2020) and Škorvánek et al., *supra* note 16, at 997, 1012-31.

the Dark Web and catching pedophiles.[24] But as this Article further argues, such publicized use of malware might also be deceptive, and the growing use of police hacking can lead to normalizing such tools in everyday police work, and the current legal framework could support such use well outside the realm of the Dark Web.[25]

A. The Road to Malware

Police forces are responsible for maintaining public safety by preventing and investigating crimes. To fulfill such a task, they must use intelligence methods of various sorts, including spying on what suspects are doing or saying.[26] In the old days, such spying was primarily conducted by stakeouts, informants, or interrogating suspects.[27] When new forms of communication enabled individuals to share messages across the land and even talk from afar, new investigatory tools were born. From letters to telegraph messages and telephone calls, the police used such forms of communication to gather evidence.[28] To catch criminals, the argument goes, the police must obtain access to the main form of communication suspects will likely use.[29]

Like the telegraph in the 19th century, wiretapping telephones became obsolete in the 21st. While phones still exist, their functionality dramatically differs from what Bell first invented.[30] Much like other technological devices, phones became computers and, more importantly, in the eyes of law enforcement, an essential tool that individuals carry with them almost constantly. While people sometimes still use mobile devices to talk, this device expanded the array of communication tools via text, recorded messages, photos, emojis, videos, and emails, among other tools, expanding how individuals exchange thoughts.

[24] *See infra* Part I.A.

[25] *See infra* Part I.B.

[26] *See* Eldar Haber, *The Wiretapping of Things*, 53 U.C. DAVIS L. REV. 733, 733-34 (2019) [hereinafter *Wiretapping of Things*].

[27] *Id.*

[28] For more on the legality of telegraph and telephone wiretapping, see *id.* at 736-44.

[29] *See id.* at 734.

[30] *See Alexander Graham Bell*, History, https://www.history.com/topics/inventions/alexander-graham-bell (last updated Aug. 25, 2023) [https://perma.cc/YUH9-4D2H].

Thus, wiretapping phone calls are becoming less practical for criminal investigation, as suspects will likely use other forms of communication within their reach.[31] Due to encryption, such communication tools also provide better secrecy for culprits to communicate, making it even more likely for them to use.[32] When investigating crimes in the 21st century, law enforcement agents thus seek access to computer communication, mainly mobile computing like mobile phones or other IoT devices.[33]

To gain such access, law enforcement agencies must find a way to probe the mobile device or the data and metadata it produced remotely, especially in cases where secrecy plays a role.[34] There are various

[31] *See* Editorial, *Eavesdropping on Internet Communications*, N.Y. TIMES (May 19, 2013), https://www.nytimes.com/2013/05/20/opinion/eavesdropping-on-internet-communications.html [https://perma.cc/4TY7-X2X6] ("The F.B.I. has long complained that it is becoming ever harder to carry out court-approved, real-time eavesdropping on criminal suspects since people are communicating without picking up a phone.").

[32] Obviously not everyone carries a smartphone, and one might argue that criminals are less likely to use such phones due to the possibility that the police might gain access to them. Still, it becomes more difficult for individuals in western society to avoid using these devices in their daily lives. For statistics on the increased use of smartphones, see Petroc Taylor, *Number of Smartphone Subscriptions Worldwide from 2016 to 2021, with Forecasts from 2022 to 2027*, STATISTA (July 19, 2023), https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide [https://perma.cc/QC35-R24M]. For more on encryption, see *infra* note 39.

[33] Smartphones are part of the IoT, which are devices or sensors that "connect, communicate or transmit information with or between each other through the Internet." This is not to argue that other computers like tablets, laptops, or PCs are no longer used. All of them could be potentially accessed with malware as well. *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 6 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/G68H-KVXL]; Škorvánek et al., *supra* note 16, at 1001. This article will focus merely on smartphones and devices within its vicinity and less on other IoT devices. For more on the legal aspects of wiretapping IoT devices, see generally Haber, *Wiretapping of Things*, *supra* note 26.

[34] This is unlike when a suspect is arrested or detained and their smartphone is taken away for inspection. Even in those cases, however, lacking cooperation from the suspect, the police might need to install malware to access the phone's history and data. In some reported cases, police officers in the UK "mugged" a suspect using their phone, navigated through the device's menus to prevent it from locking, and extracted all relevant information while it remained unlocked. Mike Peterson, *UK Police Have Resorted to 'Mugging' Criminals Using an iPhone to Bypass Encryption*, IDROP NEWS (Dec. 5, 2016, 1:12 PM), https://www.idropnews.com/news/uk-policehave-resorted-to-mugging-

potential ways to do so. One candidate for such remote access is directly by third parties, from telecommunication providers to any app developer installed and used on the suspect's phone.[35] The police might also seek direct access to data generated by suspects in various cloud storage or other servers,[36] which could also be accessible by various service providers.[37] Thus, upon a legal order, or even divulged voluntarily, the police would have to physically search the data within

criminals-using-an-iphone-to-bypass-encryption/27387 [https://perma.cc/US7J-WUXS]. For more on the constitutional aspects of compelling suspects to disclose their passwords, see generally Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019) and Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203 (2018).

[35] For instance, law enforcement agents could subpoena a third party for an online suspect's identity. They can also serve a search warrant or wiretap orders. *See* Mayer, *supra* note 4, at 577.

[36] Cloud computing could be defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." Abdella Battou, Robert B. Bohn, John V. Messina, Dr. Michaela Iorga, Eric Simmon, Michael D. Hogan & Frederic de Vaulx, *NIST Cloud Computing Program — NCCP*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/programs-projects/cloud-computing (last visited Sept. 22, 2023) [https://perma.cc/KYZ9-MBXS]. With the rise in cloud services and increased internet connectivity, people are expected to use remote servers more often to keep their data. *See* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1689 (2018) (citing JANNA ANDERSON & LEE RAINIE, PEW RSCH. CTR., THE FUTURE OF CLOUD COMPUTING 8 (2010), http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing [https://perma.cc/9GEM-6Z29] (predicting "a future in which all of us access software and share information through cloud servers rather than personal computers")).

[37] Online intermediaries often work closely with the police when criminal activities are involved. In the Apple-FBI case, while Apple refused to create a vulnerability in their system as to unlock the specific iPhone in question, they did grant the FBI access to the terrorist's Apple iCloud account. *See* Ellen Nakashima & Mark Berman, *FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup*, WASH. POST (Feb. 20, 2016), https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-forshooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html [https://perma.cc/2E3Z-34VM]; Somini Sengupta, *Concerns Arise on U.S. Effort to Allow Internet 'Wiretaps'*, N.Y. TIMES (May 16, 2013), https://www.nytimes.com/2013/05/17/business/concerns-arise-on-us-effort-to-allow-internet-wiretaps.html?ref=technology [https://perma.cc/RZ4L-PSJZ] ("Law enforcement officials regularly seek information from Web companies about the communications of their users, from e-mail messages to social network posts and chats.").

the captured device of the suspect or remotely access such data by one of the suspect's service providers.[38]

In many instances, however, such methods will be insufficient for investigation. Devices, messaging services, and many websites are becoming more secure and encrypted.[39] Traditional interception methods might not be plausible as many services use end-to-end encryption, and many intermediaries cannot aid in wiretapping practically and are not obliged by the law to do so.[40] Some culprits might

[38] *See* Rachel Bercovitz, *Law Enforcement Hacking: Defining Jurisdiction*, 121 COLUM. L. REV. 1251, 1259 (2021) (discussing the two traditional routes of data search in federal law enforcement).

[39] This claim relates to the security of devices and apps, and it is attributed at least partially to Edward Snowden's leaks. *See* Mayer, *supra* note 4, at 576. To exemplify the security of devices, mobile devices often offer the possibility of locking the device and encrypting the content while not in use. One famous case, sometimes referred to as the Apple-FBI standoff, followed the 2015 San Bernardino terrorist attack, where the FBI could not access the iPhone 5C data of Syed Farook (one of the perpetrators). Because Apple did not know Farook's password, the FBI requested the court to order Apple to change its security measures and introduce new functions to the operating system, enabling electronic input of passcodes. This would simplify the process of unlocking an iPhone through "brute force" by using the rapid processing capabilities of modern computers to try thousands or even millions of combinations. *See* Bert-Jaap Koops & Eleni Kosta, *Looking for Some Light Through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities Against "Going Dark"*, 34 COMPUT. L. & SEC. REV. 890, 896 (2018); Liguori, *supra* note 23, at 323-24; *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/E2A6-BE5M]. In addition, messaging services like WhatsApp offer end-to-end encryption; and many websites encrypt traffic in transit. Anyone else, including the owners of WhatsApp, is incapable of reading these messages. *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 990 (2018); Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, 36 BERKELEY TECH. L.J. 469, 470-71 (2022).

[40] *See* Škorvánek et al., *supra* note 16, at 1000 (making this argument). Some legislative proposals tried to oblige companies to decrypt users' data upon legal request. *See, e.g.*, N.Y. CNTY. DIST. ATT'Y'S OFF., REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY (2016), https://www.manhattanda.org/wp-content/uploads/2018/02/ENCRYPTION-2.pdf [https://perma.cc/2GNR-MPT9] (listing proposals and advocating such legislation); Press Release, Off. of Sen. Dianne Feinstein, Intelligence Committee Leaders Release Discussion Draft of Encryption Bill (Apr. 13, 2016), https://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation [https://perma.cc/A8PM-6GFE] (introducing the

use encrypted communications that lack a direct service provider, like the anonymized Tor network.[41] These developments had been generally dubbed by the intelligence and law enforcement communities as the "Going Dark" problem, suggesting that such platforms severely harm their interception capabilities.[42] It makes investigations much more complex,[43] adding another hurdle that might not be easily passed.[44] To fight against such hurdles, some states considered forcing companies to provide a "backdoor"[45] or the ability to decrypt communication upon request.[46] But aside from the various negative consequences of such a

Compliance with Court Orders Act of 2016 that would have required companies to render technical assistance or provide decrypted data, upon court order).

[41] *See* JONATHAN L. ZITTRAIN, MATTHEW G. OLSEN, DAVID O'BRIEN & BRUCE SCHNEIER, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 6 (2016), https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y [https://perma.cc/4RGN-BTAB]; THE TOR PROJECT, *supra* note 4.

[42] *See Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 1 (2015) (joint statement of Sally Quillian Yates, Deputy Att'y Gen. of the United States, and James Comey, Director of the FBI); ZITTRAIN ET AL., *supra* note 41, at 1; Bercovitz, *supra* note 38, at 1259 (describing "anonymizing software and encryption technology" as leading to the going dark problem); Liguori, *supra* note 23, at 320-25 (describing the "Going dark" debate); Škorvánek et al., *supra* note 16, at 1001; James B. Comey, Dir., FBI, Remarks Made at the Brooking Institution: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/GYD7-T53B].

[43] Encrypted data is rather useless for the police without its decryption to plaintext. *See* Kerr & Schneier, *supra* note 39, at 990-91.

[44] Such a step was dubbed by Orin Kerr and Bruce Schneier as "encryption workarounds." *See id.*

[45] In response to the going dark problem, the state might attempt to make sure that companies provide backdoors in their encrypted systems so that the government can access it when desired. For more on backdoors and their difficulties, see Koops & Kosta, *supra* note 39, at 892-94.

[46] The Clinton Administration promoted the implementation of a device called the "Clipper Chip." This chip was designed to secure voice and data messages, while also providing law enforcement agencies with the ability to decode those messages when required. It was eventually abandoned. *See generally* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995) (discussing the Clipper Chip). Still, there are democratic states that choose such a path. *See* Koops & Kosta, *supra* note 39, at 894.

move,[47] it might also not be helpful to law enforcement because criminals can use methods the government cannot compel to creating a backdoor or decrypting the communication.[48]

Here is where trojan horses might have first come into play.[49] To bypass such practical hurdles, law enforcement will likely attempt to use malware — a computer virus placed within the suspect's device, which could then send the police the data and metadata that the device produces in real-time, along with any data and metadata stored on the device or the accounts linked to the device. The malware can be installed by physically accessing a computer, remotely accessing a suspect's account,[50] or remotely infecting their device with it.[51] It is the last action, remotely installing trojan horses, which will be the focus of this Article.

While the state's use of hacking began a long time ago,[52] often for espionage purposes,[53] the scope of malware currently used by police forces in the U.S. lies much in the dark. It is not a secret that the FBI has been known to use NITs, a code name for malware, for a considerable time.[54] They have often done so to expose the identity of culprits in the

[47] *See generally* Froomkin, *supra* note 46 (discussing the negative consequences of grating governmental access to computers).

[48] *See* Koops & Kosta, *supra* note 39, at 894.

[49] *See* Nicole Perlroth, *How Spy Tech Firms Let Governments See Everything on a Smartphone*, N.Y. TIMES (Sept. 2, 2016), https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html [https://perma.cc/6APA-83TH] ("The NSO Group's capabilities are in higher demand now that companies like Apple, Facebook and Google are using stronger encryption to protect data in their systems, in the process making it harder for government agencies to track suspects.").

[50] The police can hack into a computer by covertly gaining access to it using the user's login credentials, such as their username and password. *See* Škorvánek et al., *supra* note 16, at 1008.

[51] *Id.* at 1007.

[52] *See* Liguori, *supra* note 23, at 319 ("[G]overnment hacking has been deployed in practice since at least the 1990s.").

[53] *See* Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58, 58-59 (2017) (exemplifying state vs. state hacking).

[54] At least since 2001, but perhaps even three years earlier, considering the use of Carnivore (a traffic sniffer). *See* Mayer, *supra* note 4, at 575 n.16–17; Kevin Poulson, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, WIRED (Apr. 16, 2009, 9:33 PM), https://www.wired.com/2009/04/fbi-spyware-pro [https://perma.cc/

Dark Web, which could be highly difficult without infecting them with malware.[55] A famous case is the Playpen investigation (also known as Operation Pacifier).[56] Playpen was a child pornography hosting service operating within the Tor network.[57] The only way to access it was through Tor, and one would require knowledge of the site's random string of characters, which formed its online address.[58] Lacking access to the culprits' IP addresses, police forces worldwide could not identify and bring legal action against them.[59] Tipped by a foreign agency that Playpen was misconfigured, i.e., that its IP address was publicly available and located within the U.S.,[60] the FBI obtained a search warrant, seized

NFH6-75W5]; Kim Zetter, *Everything We Know About How the FBI Hacks People*, WIRED (May 15, 2016, 7:00 AM), https://www.wired.com/2016/05/history-fbis-hacking [https://perma.cc/7CYG-5J98] (summarizing the history of FBI hacking). In the past, such a tactic was referred to as "a workbench project" and "Computer and Internet Protocol Address Verifier." *See* Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 YALE J.L. & TECH. 26, 38 (2016).

[55] *See* Škorvánek et al., *supra* note 16, at 1001. For more on the international aspects of NITs in the Dark web, see Ghappour, *supra* note 23.

[56] Another rather famous example is known as Operation Torpedo. Beginning with an investigation in the Netherlands in August 2011, law enforcement agents found out that 31-year-old Aaron McGrath was hosting three child porn sites in Bellevue, Nebraska. The FBI decided to surveil him for a year before they arrested him, and equipped with search warrants, they inserted NITs to the code of these sites and collected the IP address of those that visited it. Operation Torpedo led to several arrests both domestically and internationally. *See* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), https://www.wired.com/2014/08/operation-torpedo [https://perma.cc/J3UH-THTH].

[57] This site hosted, *inter alia*, child sexual abuse material and child sexual exploitation. U.N. OFF. ON DRUGS & CRIME, DIGEST OF CYBER ORGANIZED CRIME 108 (2021), https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook_rev.pdf [https://perma.cc/4JTD-L7Y4].

[58] Notably, Playpen amassed a base of over 200,000 users from around the world, who collectively made over 100,000 posts. Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, WASH. POST: VOLOKH CONSPIRACY (Sept. 27, 2016, 4:03 PM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant [https://perma.cc/4777-UQHW].

[59] Traditionally, the police can subpoena an Internet Service Provider for the IP address of a suspect. *See id.*

[60] *See* Mark Rumold, *Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation*, ELEC. FRONTIER FOUND. (Sept. 15, 2016), https://www.eff.org/deeplinks/2016/09/

the server hosting the site, and continued to operate it from a government facility.[61] Then, equipped with a second court order, the FBI used malware to infect visitors.[62] By doing so, the FBI could learn who visited the website through their IP address, among other details they obtained,[63] and eventually capture evidence and bring many of them to justice.[64]

The technique used within the Playpen investigation, often known as a watering hole attack,[65] is merely one example of many spyware of various sorts that the FBI has used since the beginning of the 21st century.[66] It is an intriguing use, legally speaking, because when courts approve a single warrant, they do so to infect an unlimited number of computers with malware, whereas their location could be anywhere.[67]

playpen-story-fbis-unprecedented-and-illegal-hacking-operation [https://perma.cc/2BK4-X6W4].

[61] The FBI operated the site controversially for almost two weeks, which led to much criticism later. *See id.*; Corey Rayburn Yung, *F.B.I Allowed for More Victimization by Permitting a Child Pornography Website*, N.Y. TIMES (Jan. 27, 2016), https://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/fbi-allowed-for-more-victimization-by-permitting-a-child-pornography-website [https://perma.cc/WGF2-YR3S].

[62] *See In re* Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015). Interestingly, while the warrant was broader in scope, it appears that the government deployed the NIT exclusively when a user with an active session clicked on a link to visit the "'Preteen Videos — Girls Hardcore' forum." *See* Kerr, *supra* note 58.

[63] *In re* Search of Computers that Access upf45jv3bziuctml.onion, at ¶ 33–36.

[64] While the NIT was operational under the warrant's authority, it was installed on over 1,000 visitor computers, which resulted in nearly 200 different criminal cases across the United States, all of which pertained to child pornography charges. *See* Kerr, *supra* note 58; *The Playpen Cases: Frequently Asked Questions*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whathappened (last visited Feb. 17, 2023) [https://perma.cc/U7UY-HJHS].

[65] A watering hole attack in this context involves predicting which site a user will browse and infecting it with malware before such a visit. *See* U.N. OFF. ON DRUGS & CRIME, *supra* note 57, at 108-09.

[66] Another method is a phishing attack, targeting specific individuals by sending them an electronic communication with an attachment (or link) embedded with a NIT. *See* Bercovitz, *supra* note 38, at 1260 (describing two methods that law enforcement use to deliver NITs).

[67] *See* Andrew Crocker, *Why the Warrant to Hack in the Playpen Case Was an Unconstitutional General Warrant*, ELEC. FRONTIER FOUND. (Sept. 28, 2016),

But such use of malware is not solely reserved for the Dark Web. One example of such deviation is a court's approval of physically installing a "Key Logger System" (hardware or software that captures users' keystrokes).[68] Upon receiving a court order related to suspicions of illegal gambling and loansharking activities, the police installed malware on the suspect's computer to decipher the passphrase of an encrypted file.[69] Upon this case, the police also began to use a keylogging software named Magic Lantern that could be sent by email, thus using malware from afar.[70]

Such use of malware is not merely domestic but also international in scope. Globally, one of the most significant criminal operations to date is Trojan Shield.[71] In Trojan Shield, the FBI and Australian police collaborated to run a sophisticated sting, providing criminals with cellphones (called ANOM devices) that allegedly sent encrypted messages and photos but were trojan horses, sending the data to police

https://www.eff.org/deeplinks/2016/09/why-warrant-hack-playpen-case-was-unconstitutional-general-warrant [https://perma.cc/HT6C-JQNK].

[68] Kerr & Schneier, *supra* note 39, at 997 (explaining the use of a key logger).

[69] In *United States v. Scarfo*, the agents found a suspicious file on the suspect's computer which was protected by password. Upon a warrant, they covertly installed a keylogger which later revealed the password (the prison ID number of Scarfo's father). The court later held that a traditional search warrant was sufficient due to the way the keylogger was installed. *See* 180 F. Supp. 2d 572, 581-83 (D.N.J. 2001); Kerr & Schneier, *supra* note 39, at 997 (describing the Scarfo case). Another example is the use of NITs in investigating bomb threat emails within the Dark web, known as AlphaBay. *See* U.S. DEP'T OF JUST., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S STRATEGY AND EFFORTS TO DISRUPT ILLEGAL DARK WEB ACTIVITIES 6 (2020), https://oig.justice.gov/sites/default/files/reports/21-014.pdf [https://perma.cc/W6NX-FPLM].

[70] *See* Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J.L. & TECH. 257, 275-77 (2002) (discussing keyloggers and the Magic Lantern); Bob Sullivan, *FBI Software Cracks Encryption Wall*, MSNBC (Oct. 28, 2003, 10:30 AM PST), http://www.nbcnews.com/id/3341694/ns/technology_and_sciencesecurity/t/fbi-software-cracks-encryption-wall/#V2wwfvkrLct [https://perma.cc/L8YR-KS5R].

[71] As another example, in 2020, police forces in the EU hacked into an encrypted phone network used by organized criminals around the world. Adam Nossiter, *When Police Are Hackers: Hundreds Charged as Encrypted Network Is Broken*, N.Y. TIMES (July 2, 2020), https://www.nytimes.com/2020/07/02/world/europe/encrypted-network-arrests-europe.html [https://perma.cc/USH4-FJ9V]. For more examples, see Kerr & Murphy, *supra* note 53, at 63-64.

forces around the world.[72] The operation eventually managed to intercept over 20 million messages in 45 languages and led to the arrest of at least 800 people worldwide.[73]

These spywares, however, must become more sophisticated as criminals keep finding ways to avoid detection and perhaps more importantly, operate outside of the Dark Web. Practices like the one used within the Playpen investigation, and physical limitations for installing such malware, place hurdles in fighting against many criminal activities. Law enforcement agents might thus seek something akin to a wiretap order that does not require the active involvement of the criminal or intermediaries. Such a form of NIT occurs with an exploit, i.e., a code that takes advantage of a vulnerability and accesses it from afar.[74]

Here enter relatively new hacking tools, often provided by mercenary spyware companies. One known example of such companies is the Israeli NSO Group ("NSO"), which develops spyware and markets them to governments worldwide to surveil and catch terrorists and "major criminals."[75] Pegasus, NSO's flagship spyware, can turn a mobile phone

[72] Yan Zhuang, Elian Peltier & Alan Feuer, *The Criminals Thought the Devices Were Secure. But the Seller Was the F.B.I.*, N.Y. TIMES (June 8, 2021), https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-anom.html [https://perma.cc/HCS6-Y4WA].

[73] *Id.* Another example of such use of malware is within the EU, where a joint French-Dutch collaboration led to the closing of EncroChat — a secure smartphone messaging service. Equipped with a court order, the police were able to implant a "backdoor," enabling them to intrude into the server infrastructure of an encrypted communications network, downloading information about over 32,000 phones in 121 countries. *See* U.N. Report, *supra* note 10, at 3 n.13; Peter Sommer, *Evidence from Hacking: A Few Tiresome Problems*, DIGIT. INVESTIGATION, Mar. 2022, at 1.

[74] Exploits might take various forms. Some, often called backdoors, might be deliberately placed, often by the software vendors themselves. Other weaknesses might be unintended. These flaws could be in a specific version of a device or operating system, or in a specific app. *See* Kerr & Schneier, *supra* note 39, at 1005-07.

[75] Dana Priest, Craig Timberg & Souad Mekhennet, *Private Israeli Spyware Used To Hack Cellphones of Journalists, Activists Worldwide*, WASH. POST (July 18, 2021, 8:15 PM), https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones [https://perma.cc/5A6G-2JQW]; *see also* David Pegg & Sam Cutler, *What Is Pegasus Spyware and How Does It Hack Phones?*, GUARDIAN (July 18, 2021, 12:00 PM EDT), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [https://perma.cc/8344-G9PK].

(or other computers) into a covert twenty-four-hour tracking and listening device, granting access to the data stored on the device and accounts linked to it.[76] Aside from geolocation data, Pegasus could turn the camera and the microphone on and show what the phone sees and hears in real time.[77] In its earlier versions, which date back to 2016, the deployment of Pegasus was based on social engineering: it was constructed under what is termed "spear-phishing." [78] Upon knowing the target's device, one would send them a message with an exploit link,[79] hoping they would be tricked into clicking it and be infected with the malware.[80]

These capabilities are far more advanced these days. Under what is known as "zero-click" hacks or attacks, spyware like Pegasus infiltrates systems without user interaction.[81] When the suspect's phone receives a signal, whether a message or a phone call, the malware is deployed regardless if the message was never opened or the call answered.[82] From the user's perspective, while phishing is largely avoidable with proper digital knowhow and awareness, there is no protection against zero-click attacks, even for the world's most prominent cybersecurity expert. And while other new methods for malware infection exist,[83] these zero

[76] *See* Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES (Jan. 28, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [https://perma.cc/RD3M-BWH2]; Pegg & Cutler, *supra* note 75.

[77] *See* Pegg & Cutler, *supra* note 75.

[78] *Id.*

[79] *See* BILL MARCZAK, JOHN SCOTT-RAILTON, SARAH MCKUNE, BAHR ABDUL RAZZAK & RON DEIBERT, THE CITIZEN LAB, HIDE AND SEEK: TRACKING NSO GROUP'S PEGASUS SPYWARE TO OPERATIONS IN 45 COUNTRIES 7 (2018), https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf [https://perma.cc/7Z7B-3CN9].

[80] *See* Pegg & Cutler, *supra* note 75.

[81] *Id.*

[82] *Id.* Zero-click hacks or attacks (or "zero days") are vulnerabilities without a publicly known patch or fix. *See* Koops & Kosta, *supra* note 39, at 899.

[83] Other firms may, for instance, provide a tool that infects devices when they are in proximity by taking over their WiFi connection and transmitting the trojan horse through the compromised connection. *See* Assaf Gilead, *Israeli Companies Face Trojan Horse Dilemma*, GLOBES (Dec. 27, 2021, 2:04 PM), https://en.globes.co.il/en/article-israeli-companies-face-trojan-horse-dilemma-1001396123 [https://perma.cc/ZX7J-9FJH] (exemplifying Cognyte's spyware).

clicks are currently highly attractive from a law enforcement perspective, as they require no cooperation from the suspect or intermediaries, both could be completely unaware that an attempt was even made. And as mentioned, once the phone is infected with malware, it communicates with its operator, sending it private data that could include almost anything, from passwords to contact lists, text messages, and live events.[84] If such practice is effective, culprits will be forced to get entirely off the grid for complete safety.

From theory to practice, NSO is only a drop in a growing mercenary spyware industry sea.[85] And indeed, police forces worldwide are already using these or similar services. While some never officially admitted doing so, many governments had been reported to use malware like Pegasus.[86] Specifically, Pegasus was linked to the capture of the Mexican drug lord Joaquín Guzmán Loera, also known as El Chapo, for taking down a global child abuse ring, thwarting terrorist plots, and fighting organized crime.[87]

Police hacking is becoming more prevalent not simply in authoritarian regimes but also in democratic societies. As revealed by a journalist in Israel, the home of several mercenary spyware companies, the local police had been using NSO tools to combat crime for a while,

[84] *See* MARCZAK ET AL., *supra* note 79, at 7. It is almost overwhelming (and alarming) how little attention is paid to police hacking in the context of criminal law within academic literature.

[85] For more on the mercenary spyware industry, see Ronald Deibert, *New Citizen Lab Report: Pegasus vs Predator*, CITIZENLAB (Dec. 17, 2021), https://deibert.citizenlab.ca/tag/nso [https://perma.cc/94L8-EC48] and Cooper Quintin, *Uncle Sow: Dark Caracal in Latin America*, ELEC. FRONTIER FOUND. (Feb. 10, 2023), https://www.eff.org/deeplinks/2023/02/uncle-sow-dark-caracal-latin-america [https://perma.cc/YR3Z-93U6].

[86] NSO's spyware is alleged to have been deployed by many governments worldwide, e.g., Germany, Saudi Arabia, the United Arab Emirates, Hungary, Poland, and India. Some reports also indicate some involvement in Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, and perhaps in Belgium. *See* Ronan Farrow, *How Democracies Spy on Their Citizens*, NEW YORKER (Apr. 18, 2022), https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens [https://perma.cc/9FMK-MP7Q] (quoting a former senior Israeli intelligence official stating that "German, Polish, and Hungarian authorities have admitted to using Pegasus. . . . Belgian law enforcement uses it, too, though it won't admit it"); Priest et al., *supra* note 75.

[87] *See* Bergman & Mazzetti, *supra* note 76.

well outside the Dark Web ("Israeli revelations").[88] Such revelations created a public outcry to examine the use and potential misuse of the police with these tools and to reexamine the legal framework that had enabled such a use.[89] The question was whether the state's action was permitted by Israeli law and of the level of involvement the court had in permitting such tools. Upon investigation, led by Amit Merari (Deputy Attorney General for criminal matters), the Israeli Ministry of Justice published a report on the police use of NSO's malware (the Merari Report).[90] The Merari Report found that the police used several spyware, most notably, a version of Pegasus (they called Saifan), in the investigations of various crimes, but not without a warrant.[91] While authorized, the report also found that the use of Saifan might have been broader than what was authorized under their warrant and included individuals remotely linked to a crime.[92] It also questioned how the current legal framework adequately governs the use of such malware as it is currently constructed, as such warrants were issued based on the

[88] *See* Ganon, *supra* note 11.

[89] To clarify, it is not the legality to develop such tools which was under scrutiny (at least in Israel), as companies like NSO operate openly and under the state's watching eyes through an export license. As a private company, NSO is obliged to adhere to Israeli laws and regulations, and it operates under an export license from the Defense Ministry's Defense Export Controls Agency. *See* Defense Export Control Law, 2007, SH 2105 398 (2007) (Isr.), *translated in* OFF. OF GEN. COUNS. MINISTRY OF DEF., DEFENSE EXPORT CONTROL LAW 5766–2007, at 3, 15-17 (2007), https://exportctrl.mod.gov.il/Documents/חוק%20הפיקוח%20+%20צווים%20+%20תקנות/Defense_Export_Contro_Law.pdf [https://perma.cc/2YMT-6BTU]. Even claims regarding the violation of human rights that occurred by NSO's spyware were dismissed by an Israeli district court mainly because Amnesty International, which filed the petition, failed to prove that Pegasus had been used to spy on its members. *See* Ari Rabinovitch, *Israeli Court Dismisses Amnesty's Petition Against Spyware Firm NSO*, REUTERS (July 13, 2020, 5:09 AM), https://www.reuters.com/article/us-cyber-nso-group-amnesty-idUSKCN24E1GP [https://perma.cc/LGY5-YEAS].

[90] *See* Yuval Shany, *Stay Calm and Proceed with Caution: The Merari Report on Israeli Police's Pegasus Scandal*, LAWFARE (Aug. 25, 2022, 8:01 AM), https://www.lawfareblog.com/stay-calm-and-proceed-caution-merari-report-israeli-polices-pegasus-scandal [https://perma.cc/AM8R-WVMA].

[91] *See id.*

[92] *See id.*

interpretation of the Wiretap Act, and called for new digital surveillance legislation.[93]

Domestically, it is unclear if and to what extent police forces are using malware equivalent to Pegasus and how much such use is beyond the Dark Web.[94] From what can be inferred from available data, until 2016, there were merely four federal opinions in which a NIT was requested.[95] The practice has grown considerably, and over 200 federal requests have been issued since 2016.[96] Interestingly, almost all of them are related to the Dark Web and child pornography.[97] Unlike the Israeli revelations, at least from publicly available data, it seems that the U.S. is highly conservative in its use of police hacking, reserving it almost entirely for the Dark Web and used primarily against pedophiles.[98]

To be clear, some warrant applications revealed that the FBI does act beyond the Dark Web. While almost absent from available data, there is evidence that the FBI sought to infect a computer with malware, which was allegedly used to violate federal bank fraud, identity theft, and computer security laws.[99] In such a case, the FBI asked to use malware for thirty days to extract stored data and generate user photographs and location information.[100] While the court denied such a request,[101] it exemplifies how law enforcement agents could expand their use of

[93] *See id.*

[94] *See* U.N. OFF. ON DRUGS & CRIME, *supra* note 57, at 109 (arguing that "[i]n the United States, certain features of the source code of the network investigative technique are classified and requests to reveal the technique source code have been denied, even when this denial has resulted in the dismissal of charges against defendants").

[95] *See* Mayer, *supra* note 4, at 578 n.26.

[96] To find out, I searched Westlaw for opinions that match the query "network investigative technique." Then, I examined which cases were not about child pornography. For data until 2018, see *id.* at 578.

[97] I conducted a similar search in Westlaw (as of Feb. 17, 2023).

[98] For another example of such a case, see *United States v. Laurita*, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016) (using a NIT to identify the defendant's IP address and gather evidence related to the possession and distribution of child pornography in Tor).

[99] *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

[100] *See id.*

[101] The court denied the warrant request because it was not supported by the application presented. *See id.* at 761.

malware outside of the Dark Web. But it still seems highly limited in scope and dramatically differs from Israel.

Interestingly, in recent years, law enforcement agencies in the U.S. have grown interested in using software like Pegasus for investigatory purposes.[102] In 2019, the FBI bought a Pegasus license for evaluation purposes but never used it officially in an investigation.[103] The New York Police Department also recently considered using it.[104] At least declaratively, they decided to go in a different direction.

But they did more than that. In November 2021, The Commerce Department's Bureau of Industry and Security added NSO Group and Candiru (another Israeli company), along with two other companies, one from Russia (Positive Technologies) and one from Singapore (Computer Security Initiative Consultancy PTE. LTD.), to its entry list, restricting corporations with them without a specific governmental license.[105] Effectively, these companies were barred from legally using operating systems like Windows, computers like Dell, or U.S.-based cloud servers.[106] But the fact that U.S. law enforcement does not use

[102] Notably, due to Israeli government constraints, Pegasus is not able to hack into American numbers, and thus NSO granted a different license for a malware called "Phantom." *See* Bergman & Mazzetti, *supra* note 76.

[103] *See id.*

[104] *See* Joseph Cox, *NSO Group Gave Pegasus Spyware Demo to the NYPD*, VICE (Feb. 8, 2022, 6:00 AM), https://www.vice.com/en/article/m7vp93/nso-group-pegasus-demo-nypd [https://perma.cc/P7TY-CAPY]. Reporters indicated that in 2020, NSO Group also offered the San Diego Police Department and the Los Angeles Police Department an opportunity to purchase the somewhat similar "Phantom" malware. *See id.*

[105] The entity list refers to entities that engage "in activities that are contrary to the national security or foreign policy interests of the United States." Specifically, these restrictions mean that entities like suppliers or experts cannot sell a product or transfer knowledge to these companies without a license. *See* Press Release, U.S. Dep't of Com., Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/JTJ3-MY6J]. Christopher Bing, *U.S. Blacklists Israeli Hacking Tool Vendor NSO Group*, REUTERS (Nov. 3, 2021, 4:54 PM PDT), https://www.reuters.com/technology/us-blacklists-four-companies-israel-russia-singapore-citing-spyware-2021-11-03 [https://perma.cc/Y58R-SC44].

[106] The Biden administration determined that NSO has acted "contrary to the foreign policy and national security interests of the US," and thus was federally blacklisted, effectively meaning that they are barred from buying parts and components

NSO's spyware does not mean that it is not pushing towards increased use of spyware, and much like what was revealed in Israel, perhaps such use is somehow shielded from plain sight.

To summarize, as long as communication technology becomes more secure, police forces will likely move more towards hacking into suspects' devices.[107] In that instance, the "Going Dark" problem might not be a problem. It does not matter if a suspect uses a Tor browser, Google, or any messaging app. Once the police have infiltrated their phone, other security features become meaningless. While we might still be in the dark regarding the unreported use by police forces in the U.S. of malware like that of Pegasus, it will be naïve to assume that law enforcement agencies in the U.S. will not use spyware beyond the Dark Web. And perhaps, like what occurred in Israel, we might learn the scope of such use in hindsight. Therefore, it is crucial to scrutinize whether police hacking is permissible by law and whether it should be.

B. The Legality of Police Hacking

States use hacking for various purposes, and national security is the most prominent candidate. The ability to hack into terrorist phones to stop terrorist attacks seems highly plausible given the intrusive nature of investigative techniques in this field.[108] At the same time, some

from U.S. companies, unless they have a special license. Stephanie Kirchgaessner, *Israeli Spyware Company NSO Group Placed on US Blacklist*, GUARDIAN (Nov. 3, 2021, 3:53 EDT), https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist [https://perma.cc/R5K9-A62W] [hereinafter *Israeli Spyware Company*] (quoting the commerce department having a "reasonable cause to believe, based on specific and articulated facts, that the entity [NSO] has been involved, or is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States"); *see also* Bergman & Mazzetti, *supra* note 76; Farrow, *supra* note 86.

[107] *See* Mayer, *supra* note 4, at 578 ("As security and privacy technology becomes more prevalent, law enforcement hacking will only become more commonplace.").

[108] In the context of hacking, see Greg Miller & Ellen Nakashima, *WikiLeaks Says It Has Obtained Trove of CIA Hacking Tools*, WASH. POST (Mar. 7, 2017, 7:01 PM EST), https://www.washingtonpost.com/world/national-security/wikileaks-saysit-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story [https://perma.cc/C3TB-KR7Y]. For more on various methods used by enforcement agencies for purposes of national security, see generally Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV.

governments might abuse their power to spy on individuals and use malware outside of the scope of national security, e.g., to spy on journalists, human rights activists, and state officials,[109] for reasons like political espionage,[110] or other purposes.[111]

105 (2016). This article, however, focuses on criminal enforcement and not national security.

[109] It was even reported to be used against French President Emmanuel Macron, prime minister Édouard Philippe, and many French cabinet members. *See* Angelique Chrisafis & Stephanie Kirchgaessner, *French Minister's Phone Shows Traces Linked to NSO Spyware*, GUARDIAN (July 20, 2021, 3:35 PM EDT), https://www.theguardian.com/world/2021/jul/20/french-ministers-phone-shows-traces-linked-to-nso-spyware [https://perma.cc/GD5G-4PSS]; Kirchgaessner, *Israeli Spyware Company*, *supra* note 106.

[110] As reported by the Guardian, Pegasus (along with other potential malware) was used against political figures in Spain such as the speaker of the Catalan regional parliament, Roger Torrent. Stephanie Kirchgaessner & Sam Jones, *Phone of Top Catalan Politician "Targeted by Government-Grade Spyware*,*"* GUARDIAN (July 13, 2020, 6:15 PM EDT), https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware [https://perma.cc/Y6GU-52X5]. It was also reportedly used against Indian journalists, human rights activists in Morocco, and against diplomats and senior government officials around the world. Most famously, perhaps, was the use against journalist Jamal Khashoggi's phone prior to his assassination. Dana Priest, *A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months Before His Murder, New Forensics Show*, WASH. POST (Dec. 21, 2021), https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus [https://perma.cc/SDL3-3C96]. It was also reported that there were several suspected instances of Pegasus spyware infections within official UK networks in 2020 and 2021. *See* Christopher Bing, *Watchdog Warned UK Government of Spyware Infections Inside 10 Downing Street*, REUTERS (Apr. 19, 2022, 2:27 AM PDT), https://www.reuters.com/world/uk/watchdog-warned-uk-government-spyware-infections-inside-10-downing-street-2022-04-18 [https://perma.cc/G88N-6FYN]. It was used by Mexican authorities against journalists and political dissidents and by the United Arab Emirates against a civil rights activist. *See* Bergman & Mazzetti, *supra* note 76. It was also used in Thailand against pro-democracy protesters, and activists calling for reforms to the monarchy. The malware was used against activists, academics, lawyers, and NGO workers. *See* John Scott-Railton, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert & Ron Deibert, *Pegasus Spyware Used Against Thailand's Pro-Democracy Movement*, CITIZEN LAB (July 17, 2022), https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement [https://perma.cc/Z5MV-NMV5].

[111] Pegasus, for example, was reported to be used to spy on the ex-wife of Sheikh Mohammed bin Rashid al-Maktoum, the ruler of Dubai, along with her attorneys, all because of a custody dispute. *See* Farrow, *supra* note 86.

For now, the scope of police hacking is still highly opaque. Yes, there are selective reports of some use of spyware which, aside from targeting the Dark Web, often required users' active participation or physical access to their computers. More importantly, perhaps, most of the NIT cases were of suspects caught red-handed while commencing a crime or planning one. But as inferred from the Israeli revelations, malware could expand to cases where individuals are merely suspects. And, as mentioned, with zero-click capabilities, it is done in complete secrecy and without their active participation.

Does the current U.S. legal framework that governs police hacking enable similar practices to those revealed in Israel? This Section deals with such a question by examining malware's legality for investigating criminal activities and not merely for identification purposes after a crime was commenced. Much like the current lively debate in Israel regarding the legality of such tools within the current legal framework, a similar discussion should be publicly held in the U.S., even without revelations about its actual use in the U.S.

The legality of using malware will depend on various factors. To know if legal, one must examine how the malware was delivered, deployed, and executed. Upon analysis, one can decide if a warrant is necessary for such use and, if so, which type. But a few words on jurisdiction first. Because data travels through servers in various places,[112] and suspects also might move around, malware could be installed beyond the territorial rules of a search warrant that permitted its installation.[113] Hence, judges in one state might be asked to approve malware deployment outside their legal authority's territorial reach.[114]

Since 2016, this is not a legal issue. Under an exception to the geographical limits set under Rule 41 of the Federal Rules of Criminal Procedure, which regulates the authority of federal magistrate judges to

[112] Regardless, there could be various models of cloud computing that could affect the location of data. For instance, some cloud services might split data up in a globally dispersed network while keeping them constantly in motion. *See* Schwartz, *supra* note 36, at 1687.

[113] *See* Kerr & Schneier, *supra* note 39, at 1010.

[114] Such legal authority is generally set within the Magistrates Act, codified at 28 U.S.C. § 636(a). Warrant jurisdiction is more of a problem to magistrate judges, as district court judges are not confined by these domestic territorial constraints. *See* Mayer, *supra* note 4, at 628.

issue search warrants within its jurisdiction,[115] magistrate judges are authorized to issue warrants that might exceed their territorial boundaries.[116] This exception becomes highly relevant when conducting techniques to identify culprits within anonymized networks like Tor, where the agent seeks to find these criminals but cannot know beforehand where and who they are.[117] Jurisdiction is thus not a barrier to police hacking, at least not from a domestic perspective.[118]

The legality of police hacking begins with the Fourth Amendment, the most obvious candidate for such legal oversight. The Fourth Amendment is generally constructed of two clauses. The first clause, often referred to as the Reasonableness Clause, grants people the right "to be secure in their persons, houses, papers, and effects" and protects them against "unreasonable searches and seizures."[119] It does not forbid all searches and seizures but rather unreasonable ones.[120] A Fourth

[115] *See* FED. R. CRIM. P. 41.

[116] *Id.* r. 41(b)(5) (authorizing a magistrate judge "in any district where activities related to the crime may have occurred" to issue warrants outside their jurisdiction which is within a U.S. territory, possession, commonwealth, or premises used by a U.S. diplomatic or consular mission). Additionally, it grants permission to magistrate judges to issue a warrant for remote access to search electronic storage devices and obtain or duplicate electronically stored information that may be related to criminal activity when the location of the device or information has been technologically concealed. *See id.* r. 41(b)(6)(A). It also creates an exception "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." *Id.* r. 41(b)(6)(B).

[117] *See* Bercovitz, *supra* note 38, at 1265-66.

[118] The international level is complex and lacking any agreements with the state that such use might occur in, which might mean that the court's authority is not supported constitutionally and statutorily. For more on the international aspects of NITs, see Ghappour, *supra* note 23, at 1106-07.

[119] U.S. CONST. amend. IV. One of the challenges greatly debated in court proceedings and academic literature is what constitutes "reasonable." *See, e.g.*, Flippo v. West Virginia, 528 U.S. 11, 12-15 (1999) (discussing reasonable expectation of privacy in a cabin at a state park); Minnesota v. Olson, 495 U.S. 91, 98-99 (1990) (holding that an overnight guest had a reasonable expectation of privacy in a host's home); Stoner v. California, 376 U.S. 483, 488-89 (1964) (warrantless search of a hotel room violates a reasonable expectation of privacy); Henry F. Fradella, Weston J. Morrow, Ryan G. Fischer & Connie Ireland, *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 338-42 (2011) (summarizing empirical research on reasonable expectations of privacy).

[120] *See* Terry v. Ohio, 392 U.S. 1, 9 (1968).

Amendment search occurs when an individual exhibits a subjective expectation of privacy, and society recognizes such expectation as "reasonable."[121] The second clause, often referred to as the Warrant Clause, specifies the form and content of warrants.[122] If considered a search, the police need to obtain a warrant supported by probable cause, i.e., demonstrate a reasonable basis to believe that the information sought is relevant and material to an ongoing investigation[123] while meeting the particularity requirement.[124] If there is no search, then the Fourth Amendment does not apply.

The applicability of the Fourth Amendment to malware might not be clear-cut.[125] Not every enforcement action will automatically count as a

[121] Known also as the "reasonableness test." *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[122] For more on the meaning and history of the Fourth Amendment, see generally Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 552 (1988); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999); Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197 (1993); Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925 (1997).

[123] *See* U.S. CONST. amend. IV.

[124] The particularity requirement for warrants ensures that "warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927); *see also* Stanford v. Tex., 379 U.S. 476, 485 (1965). The particularity requirement was set because of past abusive general warrants. *See* Steagald v. U.S., 451 U.S. 204, 220 (1981).

[125] A Fourth Amendment search traditionally occurs physically: at a specific location or on the person being searched; in malware, it might make things trickier. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 331-33 (2015). Notably, the intentions of its framers are generally in dispute. Some argue that the Fourth Amendment was enacted to impose a "warrant preference rule" favoring or mandating searches under a specific warrant. *See* Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 822-26 (1994); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 584 (2008). Others argue that the Fourth Amendment was intended to reduce or limit the use and scope of warrants. *See* AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 64-77 (1998); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757, 759 (1994); Akhil Reed Amar, Terry *and Fourth Amendment First Principles*, 72 ST. JOHN'S L. REV. 1097, 1097-98 (1998).

"search." Under the reasonableness test, we must examine if the suspects subjectively expected that their computer or mobile phone was private and if society objectively assures such expectation as a reasonable one. Even if considered a search, one must also assess if there are any specific exceptions to the Fourth Amendment's protection,[126] perhaps most notably, the third-party doctrine.[127] This doctrine,

[126] For instance, under what was termed by some scholars as the *container doctrine*, the Supreme Court announced that enforcement agencies, lacking any exigent circumstances supporting an immediate search, were generally required to obtain a warrant for a container search generally. *See* Arkansas v. Sanders, 442 U.S. 753, 763-64 (1979); United States v. Chadwick, 433 U.S. 1, 15 (1977); Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1414-26 (2010). But there are many exceptions to the container doctrine, which include, *inter alia*, exigent circumstances, consensual searches, the Terry stop and frisk search (which requires reasonable suspicion rather than probable cause), items that are in plain view during searches, provided that officers encounter this evidence during their authorized search and that the incriminating nature of the evidence is "immediately apparent" (Maryland v. Macon, 472 U.S. 463 (1985)), and airport and courthouse searches. *See generally* Terry v. Ohio, 392 U.S. 1 (1968) (holding that it could be permissible under the U.S. Constitution for police officers to "stop and frisk" an individual if they have a reasonable suspicion that the person is carrying a weapon and is engaged in criminal activity); Benjamin T. Clark, *Why the Airport and Courthouse Exceptions to the Search Warrant Requirement Should Be Extended to Sporting Events*, 40 VAL. U. L. REV. 707, 715-23 (2006) (explaining search warrant exceptions). For more on the plain view doctrine in the digital age, see generally Haber, *Wiretapping of Things*, *supra* note 26, at 753-54 and Andrew Vahid Moshirnia, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609 (2010). In terms of evidence, if the search was not authorized, there could still be exceptions to the exclusionary rule. One such exception is "bad faith." *See* United States v. Torres, No. 5:16-cr-285, 2016 U.S. Dist. LEXIS 122086, at *17 (W.D. Tex. Sept. 9, 2016) (While the court held that the use of a NIT was a Fourth Amendment search, those involved had not "acted in bad faith when they respectively sought and issued [it]").

[127] Forged in a series of Supreme Court cases in the 1970s, one of the main exceptions is the third-party doctrine which exempts protection for information that was voluntarily shared with a third-party. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018) (holding that the Fourth Amendment applies when government agents "accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements"); Riley v. California, 573 U.S. 373, 381(2014) (holding that a warrant was generally required to search the contents of a cell phone); United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring) (reaffirming the principle that physical invasion on personal property to gather information by the government is a search. Notably, Justice Sotomayor in concurrence noted that "it may be necessary to

however, might become less relevant in the use of malware as the information sharing is not likely made through a third party. If the data is within one's phone and that is where the police want to obtain it directly from, then the doctrine will not apply.[128]

The examination of the Fourth Amendment begins with the delivery and exploitation of the malware, not considering its execution for now. Such delivery and exploitation processes could already implicate the Fourth Amendment,[129] mainly because they will likely be considered trespass. Indeed, malware like Pegasus is placed remotely; hence the question of trespass under the Fourth Amendment might become more challenging in opposition to capturing one's computer and installing it after its seizure.[130] But as this malware and its kind are reported to be installed without the user's active participation, such action is

reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); United States v. Knotts, 460 U.S. 276, 284-85 (1983) (holding that warrantlessly tracking a beeper that only traveled through public areas did not violate the Fourth Amendment); Smith v. Maryland, 442 U.S. 735 (1979) (holding that there was no reasonable expectation of privacy for phone numbers a person dialed, as they were conveyed to the phone company); United States v. Miller, 425 U.S. 435 (1976) (holding that there is no reasonable expectation of privacy in financial records maintained by one's bank); Kyllo v. United States, 533 U.S. 27 (2001) (holding that warrant was required for the government to use a thermal imaging device). For more on *Carpenter*, see Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 YALE L.J.F. 943 (2019); *see also* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1871 (2016); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 829-30 (2004); Mayer, *supra* note 4, at 600-02; Neil Richards, *The Third Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1466-80 (2017); Daniel Solove, Carpenter v. United States, *Cell Phone Location Records, and the Third Party Doctrine*, TEACHPRIVACY (July 1, 2018), teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine [https://perma.cc/6NFY-TLW9].

[128] *See* Orin Kerr, *Remotely Accessing an IP Address Inside a Target Computer Is a Search*, WASH. POST: VOLOKH CONSPIRACY (Oct. 7, 2016, 3:42 PM EDT), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search [https://perma.cc/M498-MF88].

[129] *See* Mayer, *supra* note 4, at 584-86; Škorvánek et al., *supra* note 16, at 1030-31.

[130] Under a property-based analysis, physical interaction with a suspect's device clearly invokes the Fourth Amendment as a physical trespass to obtain data is a search. *Riley*, 573 U.S. at 401; *Jones*, 565 U.S. at 406-11; Mayer, *supra* note 4, at 594-95.

inherently trespassory.[131] In addition, as the malware circumvents technology to bypass the security protections, it should trigger Fourth Amendment protection.[132] Finally, even without holding that such action is trespassory, the Fourth Amendment protects people's privacy, not property, thus normative people reasonably expect that their phones are protected from intrusion by police officers.[133]

Thus, even if the malware is installed remotely and does not collect anything, it should constitute a search.[134] While some courts mistakenly ruled that the Fourth Amendment is not invoked when the police use a NIT to collect an IP address,[135] as other courts correctly ruled, it should

[131] Penney and Schneier further offered a "network trespass theory," arguing that accessing a network and using it to hack or stage an attack on users of that network is a trespass on the network itself (aside from the target users) and, therefore, should invoke liability under the Computer Fraud and Abuse Act ("CFAA"). *See* Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C § 1030); Penney & Schneier, *supra* note 39, at 478.

[132] Such violations might be even more evident with zero-click malware like NSO's tools, as they circumvent the technology. *See* Mayer, *supra* note 4, at 616 (arguing that "when a person circumvents a technical safeguard on a computer system, that constitutes a [CFAA] violation").

[133] The traditional trespassory violation of property to constitute a Fourth Amendment search was broadened in 1967. In *Katz*, police officers used a listening device attached to the outside of a public telephone booth, enabling them to hear one end of the target's phone conversation. In that case, even without a trespass, the Fourth Amendment was interpreted to protect the suspect's privacy interests. *See* Katz v. United States, 389 U.S. 347, 353 (1967). Thus, at least since 1967, an actual trespass is not necessary to establish a constitutional violation under the Fourth Amendment. *See, e.g.*, United States v. Karo, 468 U.S. 705, 713 (1984) (granting a warrant to install a locating beeper); Oliver v. United States, 466 U.S. 170 (1984) (holding that the area outside a property owner's curtilage is not a search within the scope of the Fourth Amendment). Under this stand, the Fourth Amendment protects people's privacy, not property. *See* Warden v. Hayden, 387 U.S. 294, 304 (1967) ("[T]he principal object of the Fourth Amendment is the protection of privacy rather than property.").

[134] *See* Arizona v. Hicks, 480 U.S. 321, 325 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable."); United States v. Torres, No. 5:16-cr-285, 2016 U.S. Dist. LEXIS 122086, at *9-10 (W.D. Tex. Sept. 9, 2016) (holding that the use of NITs are a Fourth Amendment search); Kerr, *supra* note 58.

[135] *See* United States v. Werdene, 188 F. Supp. 3d 431, 443-44 (E.D. Pa. 2016) (finding that the NIT that was installed in Werdene's computer to reveal his IP address was not a Fourth Amendment search, as he did not have a reasonable expectation of privacy in that IP address); U.S. v. Matish, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016) (reaching a similar conclusion); Kerr, *supra* note 58; Mayer, *supra* note 4, at 596.

constitute one. For the malware to discover the suspect's IP address, it must *enter* the computer first, thus invoking the Fourth Amendment even if it only obtained metadata.[136] In other words, there should be little doubt that it constitutes a Fourth Amendment search when the government hacks into a computer without the users' consent, and the mere use of malware necessitates judicial review.[137]

If courts reject such legal interpretation, they must turn to examine if executing the malware and sending back data implicates the Fourth Amendment.[138] Here it might depend on the content-metadata dichotomy, as the latter might not be fully protected under the Fourth Amendment.[139] If metadata, and the court wrongly holds that nothing in the entire process implicates the Fourth Amendment (including no reasonable expectation of privacy within the metadata), the court must turn to assess if the police qualify for an Electronic Communications Privacy Act's pen register/trap and trace order.[140] If content, such

[136] *See* United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016); Kurt C. Widenhouse, *Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found*, 13 J. BUS. & TECH. L. 143, 160 (2017).

Regardless, as mentioned, metadata might also be protected under the Fourth Amendment in some instances. *See supra* note 127 and accompanying text.

[137] *See* Mayer, *supra* note 4, at 577, 582, 589 (noting that while some of the district courts that have considered the issue have held that such hacking is not necessarily a Fourth Amendment search, it should count as one. He further notes that each of the four steps in hacking — delivery, exploitation, execution, and reporting — could potentially trigger Fourth Amendment protections).

[138] *See id.* at 589; Škorvánek et al., *supra* note 16, at 1030.

[139] *See* Škorvánek et al., *supra* note 16, at 1030.

[140] The Electronic Communications Privacy Act ("ECPA") of 1986 regulates wiretaps (18 U.S.C. §§ 2510–23), stored communications and subscriber information (18 U.S.C. §§ 2701-13), and pen registers and trap & trace devices (18 U.S.C. §§ 3121-27). Under the ECPA, the government can obtain certain types of metadata with a court order based on a lower standard of evidence than a warrant based on probable cause. This type of court order is known as a "pen register/trap and trace" order or a "2703(d)" order, and it requires the government to show "specific and articulable facts" that the information sought is relevant and material to an ongoing criminal investigation. A pen register is a device that records the numbers dialed for outgoing calls from the target phone. A trap and trace device captures the phone numbers for calls made to the target phone. *See* 18 U.S.C. § 3127; Stephen Smith, *The Cell Phone Donut Hole in the Tracking Device Statute*, 14 FED. CTS. L. REV. 1, 7-11 (2021) (explaining pen register/trap and trace); *see also* Škorvánek et al., *supra* note 16, at 1032. Originally, the pen register and trap and trace statute were

execution is a Fourth Amendment search, and a warrant is necessary. Without such authorization, the police might violate the primary federal anti-hacking statute (the Computer Fraud and Abuse Act or CFAA).[141] Such violations might be even more evident with malware like the NSO's zero-click malware tools, as they circumvent the technology.[142]

But some legal procedures might be different in the use of spyware. Some factors could change the type of warrant necessary. For content and metadata, there are two relevant "traditional" methods for obtaining electronic evidence under U.S. law, divided into data at rest and communication in transit.[143] As established, the baseline is a Fourth Amendment warrant. The first deviation from the baseline could be when the malware allows searching stored data on a device.[144] The type of warrant required for such remote data searches might differ depending on various factors. If the data is extracted directly from a device, it is generally not stored by a third-party service provider, thus the Fourth Amendment applies, not the Stored Communications Act ("SCA").[145] But if upon execution, the police search content which is not

directed to telephones but has been expanded under the Patriot Act to dialing, routing, addressing, and signaling information of communications, including dialed calls, IP addresses, and email headers. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 21I, 115 Stat. 272, 290; U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 51 (2018), https://www.justice.gov/archives/ag/page/file/1326061/download [https://perma.cc/33K7-B7Q6].

[141] *See* Act of Oct. 16, 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C § 1030). Notably, while the CFAA explicitly exempts law enforcement investigations from its regulatory scheme, but only when they act lawfully and upon proper authorization. *See* 18 U.S.C. § 1030(f) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

[142] *See* Mayer, *supra* note 4, at 616 (arguing that "when a person circumvents a technical safeguard on a computer system, that constitutes a [CFAA] violation").

[143] To be precise, there are four statutes that regulate electronic surveillance within the realm of law enforcement: The Wiretap Act, the Stored Communications Act, The Cloud Act, and the Pen Register Act. *See supra* note 140.

[144] *See* Škorvánek et al., *supra* note 16, at 1035-36.

[145] *See* 18 U.S.C. §§ 2701-12; Bercovitz, *supra* note 38, at 1261 ("While the SCA regulates compelled disclosure orders, there is no analogous statute for NIT searches."). The SCA sets the rules to obtain customer data held by internet service providers. When

stored locally but rather in remote servers (in the so-called "cloud"),[146] which could be domestic or international, then it must follow the requirements set under the Clarifying Lawful Overseas Use of Data ("CLOUD") Act (which amended the SCA).[147]

But compliance with the CLOUD Act might not be so simple. Zero-click malware relies on a specific vulnerability in the suspect's device or app, whichever is vulnerable. To avoid breaking the law in other jurisdictions and to comply with the CLOUD Act, the police must first

needed to investigate, law enforcement agents would either seize the device and directly search it or ask their service provider. Falling under the SCA requires the government to obtain a warrant or court order for such access unless the user grants consent. 18 U.S.C. § 2703; Bercovitz, *supra* note 38, at 1259. For content data stored longer than 180 days, the government can obtain a court order with a lesser burden of proof or secure an administrative subpoena. *See* 18 U.S.C. §§ 2703(b)(1)(B), 2703(d).

[146] Schwartz, *supra* note 36, at 1682 ("Data are moving from our personal devices, such as laptops and phones, and onto different configurations of remotely managed servers.").

[147] Among other things, the Act expanded and clarified the authority of U.S. law enforcement to obtain electronic communications and data stored overseas. *See* Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, 2018 U.S.C.C.A. N. (132 Stat.) 1213. Such amendment to the SCA was made following a legal controversy in the Microsoft case, dealing with the government's right to access data stored on servers located in other countries, and more specifically whether the U.S. government could force Microsoft to turn over email stored on a server in Ireland as part of a criminal investigation. *See* Microsoft Corp. v. United States, 829 F.3d 197, 201-02 (2d Cir. 2016). Under this Act, U.S.-based service providers are required to "preserve, backup, or disclose" electronic communications content that relates to one of their customers or subscribers within their reach, regardless of the location of such content. What matters is the service provider's primary location (the U.S.), not where the content is stored. *See* 18 U.S.C. § 2713; Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J.F. 1029, 1035-36 (2019). The Act also empowered the government to enter into a new series of bilateral executive agreements to expedite law enforcement cooperation. *See* REBECCA WEXLER, THE CLOUD ACT AND THE ACCUSED 14 (2022), https://s3.amazonaws.com/kfai-documents/documents/a6b5edd74f/Wexler---CLOUD-Act---v04.pdf [https://perma.cc/D2ZE-HFX9]. With this Act, the use of malware could bypass another country's prerogative over a server. The use of malware aids in overriding jurisdictional challenges, so police officers no longer rely on court decisions in other countries that might not approve a warrant when conducting an international investigation. On the other hand, it could also violate the sovereignty of other nations and threaten international relations. *See* Ghappour, *supra* note 23, at 1083-87. *But see* Kerr & Murphy, *supra* note 53, at 61-62 (skeptical of Ghappour's argument regarding international relations).

find a vulnerability that is linked to a U.S.-based company. It could be the device, e.g., iPhone (but not Samsung or Xiaomi). It could be the operating system, e.g., iOS, Android, and Microsoft's Windows phone (but not Blackberry and Ubuntu Touch). And it could be any U.S.-based app or any non-U.S. one. If such a company is not linked to the U.S., it will be beyond the subpoena of U.S. courts, which must use international collaborations so as not to commit a crime in a different country by doing so.[148]

And it is not merely a legal but also a practical problem. Zero-clicks are often targeted at a specific device manufacturer or an app that must be installed on the suspect's phone. How can the state ensure that the suspect uses a vulnerable device or app? Would (and could) the state ban using a specific phone or a messaging app that is not likely to be vulnerable? While some advocated that the state become its own supplier,[149] it still needs to work with various spyware mercenaries and

[148] *See* RESTATEMENT (THIRD) OF THE FOREIGN RELS. L. U.S. § 432(2) (1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); Schwartz, *supra* note 36, at 1709 ("For the U.S. government to carry out a search or seizure on foreign soil without the cooperation of the local government would probably constitute a crime under local law, something U.S. government agents would be reluctant to do."). Such collaboration is often commenced under global, regional, and bilateral treaties. *See* Kerr & Murphy, *supra* note 53, at 61. For crimes punishable in both jurisdictions, states often sign a mutual legal assistance treaty — a bilateral treaty binding the parties' assistance in criminal investigations. *See generally* Sarit K. Mizrahi, *The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users During the Course of Criminal Investigations in Canada and the United States*, 25 TUL. J. INT'L & COMPAR. L. 303, 345 (2017) (discussing human rights and cloud access); Wexler, *supra* note 147 (discussing the CLOUD Act and its history). Also, while such collaboration could theoretically occur outside of the scope of the Fourth Amendment as it does not generally apply outside of the U.S., it could still apply if it involves a U.S. person or someone with substantial connections to the U.S. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265-71 (1990) (holding that the Fourth Amendment's protection against unreasonable searches and seizures does not apply to non-citizens outside the U.S.); Schwartz, *supra* note 36, at 1709-10. But it will not necessarily protect noncitizens within the U.S. *See* Bercovitz, *supra* note 38, at 1273-74.

[149] *See* Kevin Bankston, *Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors*, LAWFARE (June 14, 2017, 1:00 PM), https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors [https://perma.cc/3EP9-FAXF].

largely depends on the market. This is a crucial element in the ability of the state to access all devices.

Going back to the legal aspects, the second deviation from the Fourth Amendment baseline is the real-time interception of content. Such an act will be considered wiretapping, requiring a super-warrant,[150] with a higher threshold than probable cause.[151] Wiretapping could be used for any content transferred between users, for opening their mic,[152] and turning on their camera.[153] It will fall under wiretapping if it is not metadata and is transferred in real-time. If the exact location of such interception is unknown, the court must ensure that the device is within the U.S., at the least.[154]

Such use is not fictional. Malware like Pegasus was reported to open mics and cameras of devices and transmit real-time electronic communication.[155] The use of malware, specifically NSO's Pegasus, is currently litigated in various contexts. One of the ongoing cases involves exploiting a vulnerability in WhatsApp to monitor WhatsApp users.[156] WhatsApp and its parent company Facebook (now Meta), filed

[150] *See* 18 U.S.C. §§ 2510-11, 2518; Škorvánek et al., *supra* note 16, at 1041.

[151] Aside from approval from high-ranking officials and restriction to pre-listed predicate felony offenses, the police will have to demonstrate that investigative procedures are inadequate or have failed and that they will ensure that the wiretapping will be conducted in a way that minimizes the interception of non-pertinent communications. They will also have to describe the nature and location of the communication to be intercepted and set time limits on the interception. *See* 18 U.S.C. § 2518(1)(b); Haber, *Wiretapping of Things*, *supra* note 26, at 763-64; Mayer, *supra* note 4, at 597 (arguing that it is rather obvious that such actions will trigger the wiretap act with its heightened super-warrant protection).

[152] *See* 18 U.S.C. § 2510(2) (oral communication); Škorvánek et al., *supra* note 16, at 1050.

[153] *See* Škorvánek et al., *supra* note 16, at 1055-56 (making this argument for webcams while exemplifying with court decisions). From a warrant request, we can learn that the official reason for such "photo monitoring" (in the words of the state) is to "identify the location of the TARGET COMPUTER and identify persons using the TARGET COMPUTER." *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013).

[154] *See* 18 U.S.C. § 2518(3); Škorvánek et al., *supra* note 16, at 1047-48.

[155] *See* Bergman & Mazzetti, *supra* note 76.

[156] WhatsApp argued that the attack involved a malicious code that was sent over the WhatsApp message service network to exploit a flaw. The attack gave full access and control over victims' smartphones remotely. *See The NSO WhatsApp Vulnerability — This*

a lawsuit against NSO Group and its parent company Q Cyber Technologies,[157] while the United States joined with an amicus brief supporting WhatsApp.[158] Apple followed suit and sued as well.[159] And following such controversies, Congress even considered allowing citizens and U.S. companies to sue foreign nations for cyberattacks.[160]

To clarify, these lawsuits are directed against the company for making such malware and breaking their terms of service (hacking into their systems to install spyware), thus potentially breaking the CFAA.[161] This is crucial, as it does not directly tackle the use of law enforcement agencies, or anyone else, but rather the practice of spyware companies like NSO. Are they liable under the CFAA for violating terms of service? Generally, while this was highly questionable in the past,[162] the Supreme Court's interpretation of the CFAA in *Van Buren* suggests that it is not

Is How It Happened, CHECK POINT RSCH. (May 14, 2019), https://research.checkpoint.com/2019/the-nso-whatsapp-vulnerability-this-is-how-it-happened/ [https://perma.cc/3JHJ-E8JX]; Penney & Schneier, *supra* note 39, at 481.

[157] *See* Complaint & Demand for Jury Trial at 1, WhatsApp, Inc. v. NSO Grp. Techs. Ltd., No. 3:19-cv-07123-JSC, 2019 WL 5571028 (N.D. Cal. Oct. 29, 2019); Stephanie Kirchgaessner, *NSO Group Points Finger at State Clients in WhatsApp Spying Case*, GUARDIAN (Apr. 7, 2020, 1:13 PM EDT), https://www.theguardian.com/world/2020/apr/07/nso-group-points-finger-at-state-clients-in-whatsapp-spying-case [https://perma.cc/3BLM-HANL]. For a comprehensive analysis of this lawsuit, see Penney & Schneier, *supra* note 39, at 475-87.

[158] Among other things, the state argued that the NSO Group's conduct violates the U.S. Computer Fraud and Abuse Act ("CFAA"), and that its actions threaten national security and international relations by allowing foreign governments to engage in surveillance of U.S. citizens and officials. *See* Complaint & Demand for Jury Trial at 2, *WhatsApp, Inc.* (N.D. Cal. Oct. 29, 2019).

[159] *See* Nicole Perlroth, *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*, N.Y. TIMES (Nov. 23, 2021) [hereinafter Perlroth, *Apple Sues Israeli Spyware Maker*], https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html [https://perma.cc/L69P-D7VM].

[160] *See* Homeland and Cyber Threat Act, H.R.1607, 117th Cong. (2021).

[161] Within the making of the malware, when the private company had to find an exploit for them to create the malware later be used by NSO's clients, they must use the device or the app to find it. These devices and apps will likely have terms of service, and by finding the vulnerability, even before the actual use of the malware, these companies violate these terms of service.

[162] *See, e.g.*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010) (arguing that courts might narrowly interpret the CFAA in light of existing doctrines).

a violation of the act.[163] But the potential violation of the CFAA remains to be seen. In return, NSO is attempting to use either common law immunity (in the Apple case) or the Foreign Sovereign Immunities Act (in the WhatsApp case), which could grant them a liability shield as foreign nations.[164] And as a business, it is not likely to be considered a foreign nation; thus, such a defense is invalid,[165] as the Supreme Court recently affirmed.[166]

These are not the only pending cases revolving around spyware, and we will likely see more if the practice continues.[167] But overall, it seems that police hacking is governed by various laws and regulations that set the playing field of how the police can access one's computer from afar. But much like in Israel, the legal framework was never designed for police hacking. The current legal framework is not yet well-tailored to properly balance enforcement needs and the negative implications of

[163] Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021); *see also* Penney & Schneier, *supra* note 39, at 483.

[164] The WhatsApp case refers to a 2019 lawsuit where WhatsApp accused the Israeli firm NSO of distributing spyware to about 1,400 devices through its servers, violating state and federal laws. NSO countered by claiming they were employed by undisclosed foreign governments and thus immune. *See* Andrea Vittorio, *Meta, Apple Spyware Lawsuits Test NSO's Foreign Hacking Shields*, BLOOMBERG L. (June 15, 2022, 2:10 AM), https://news.bloomberglaw.com/privacy-and-data-security/meta-apple-spyware-lawsuits-test-nsos-foreign-hacking-shields [https://perma.cc/ZM6Q-YGQ4]; William S. Dodge, *NSO v. WhatsApp: Should the Solicitor General Recommend Allowing Foreign Corporations to Claim Immunity?*, JUST SECURITY (June 9, 2022), https://www.justsecurity.org/81843/nso-v-whatsapp-should-the-solicitor-general-recommend-allowing-foreign-corporations-to-claim-immunity [https://perma.cc/Z4DC-MD93].

[165] *See* Dodge, *supra* note 164.

[166] *See* Nate Raymond, *U.S. Supreme Court Lets Meta's WhatsApp Pursue "Pegasus" Spyware Suit*, REUTERS (Jan. 9, 2023, 8:15 AM PST), https://www.reuters.com/legal/us-supreme-court-lets-metas-whatsapp-pursue-pegasus-spyware-suit-2023-01-09 [https://perma.cc/KG7R-5ZKL].

[167] In another case, the Electronic Frontier Foundation had filed a lawsuit on behalf of Loujain al-Hathloul, a Saudi political activist, against the company that enabled the hacking (DarkMatter) and former U.S. officials who were allegedly involved in the hacking. *See* Complaint and Demand for Jury Trial at 8, Alhathloul v. DarkMatter Grp., No. 3:21-cv-01787-IM, 2023 WL 2537761 (D. Or. Dec. 9, 2021); Marieke Wijntes, *Saudi Activist Sues 3 Former U.S. Officials over Hacking*, NBC NEWS (Dec. 10, 2021, 6:08 AM PST), https://www.nbcnews.com/tech/security/saudi-activist-sues-3-former-us-officials-hacking-rcna8349 [https://perma.cc/QT5C-7KWF].

police hacking for society. And much like what occurred in Israel, police forces around the U.S. might try to use this framework to deploy malware for various criminal activities and not merely those in the Dark Web, that is, if they are not doing so already. As Part II argues, this trojan horse must be stopped, for now at least, in every state that values human rights and liberties. And then it must be regulated.

II. THE HORSE THAT NEEDS REGULATING

Frank Easterbrook was wrong. Not only that the "law of the horse" argument was often proven invalid in many instances,[168] it is also far from being the case when dealing with police hacking. Trojan horses must be directly and appropriately regulated, as their use is not similar to wiretapping or accessing stored communication. As revealed in Israel, the police use of such malware could become normalized under existing statutes ill-suited to untangle the complexity of granting real-time access to one's thoughts and feelings,[169] the "sum of an individual's private life."[170] Such interpretation could grant police officers the ability to take pictures, record videos, or open the microphones of individuals, simply because they are suspected of criminal activity.

As this Part further argues, the first stage in regulating police hacking is going a step back and placing a moratorium on most of its forms. Then, upon a better understanding of the ramifications and analysis of the safeguards that must be placed, policymakers can create a just legal framework to govern such practice. It must be constrained to a limited set of criminal activities, for a brief period, limited in its technological and institutional abilities, and executed under real-time and ex-post oversight. Before Part II.B makes such a proposition, the first part will discuss the pitfalls in the current governance of police hacking while emphasizing its negative impact on human rights and liberties along with other externalities policymakers must consider.

[168] For criticism on Easterbrook's argument, see generally Lessig, *supra* note 18.

[169] *See* U.N. Report, *supra* note 10, at 5 ("There are strong arguments that tools such as Pegasus, which enable unfettered intrusions into people's lives and can even reach into their inner thoughts, could affect the essence of the right to privacy and interfere with the absolute rights to freedom of thought and opinion.").

[170] Riley v. California, 573 U.S. 373, 394 (2014).

A. *Human Rights, Liberties, and Externalities*

There should be little doubt that covertly installing malware in suspects' computers for criminal investigations violates human rights and liberties. Such action will always be an issue in the interplay between personal safety and human rights and liberties. But while the conflict between protecting individual privacy and liberty and utilizing cutting-edge technology by law enforcement will likely remain a persistent issue,[171] unlike Easterbrook's argument, not all technologies are similar, and many require a different analysis.

The first part of such interplay is thus enforcement needs. As previously argued, there is little doubt that enforcement agencies must keep up with culprits. They are not likely to be left in the dark when criminals deploy encrypted communications for their benefit. The use of malware is essential in the Dark Web, whereas traditional investigation techniques could be irrelevant, especially when serious crimes like child pornography are committed. It could also become more critical in other criminal cases outside the Dark Web, where enforcement agencies must investigate criminal activities that could be discovered via such a tool. Malware like Pegasus might aid in the fight against crime, and in the words of NSO, it has already saved "thousands of lives over recent years."[172]

But enforcement needs are only part of the interplay. When policymakers, and in turn courts, allow police officers to hack into the most intimate device that individuals carry, they must consider the potential harm such authorization could lead to the individual and society, as further explored.

It begins with the right to privacy,[173] as investigation techniques are obviously in the greatest tension with it. Spying on an individual violates

[171] *See* United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

[172] While NSO is obviously not impartial, such tools could clearly aid in finding culprits. *See* Stephanie Kirchgaessner, Nick Hopkins & Oliver Holmes, *WhatsApp 'Hack' Is Serious Rights Violation, Say Alleged Victims*, GUARDIAN (Nov. 1, 2019, 10:14 AM EDT), https://www.theguardian.com/technology/2019/nov/01/whatsapp-hack-is-serious-rights-violation-say-alleged-victims [https://perma.cc/7AM5-4XTV].

[173] Legal mechanisms, at both the federal and state levels, safeguard the right to privacy. Within the federal framework, the protection of privacy is partly based on the Court's interpretation of the Bill of Rights, primarily encompassing the First, Third,

privacy of the highest magnitude, as tools like Pegasus can grant access to almost every data point about them. It is almost the farthest from being "let alone."[174] The Fourth Amendment's "reasonableness test" was born out of similar privacy concerns involving wiretapping,[175] and the wiretap statute was born as a result of such practices.[176] Thus when discussing malware, in which wiretapping is only part of what it enables, it might become even more intrusive and necessitate a new discussion and evaluation. It also affects the privacy of others, from those who communicated with the suspect to those currently around the camera or microphone if the police opened them.[177] It will impact one's desire to use innovative technologies and the ability to retreat into one's domain, which was initially freed from unreasonable governmental intrusion.[178]

Fourth, and Fifth Amendments. *See* U.S. CONST. amends. I, III-V. The right to information privacy, which involves preserving one's authority over their personal information, is federally regulated under a sectoral approach alongside state-level regulations. This approach provides protection for specific types of data within a particular industry or context where data collection or usage occurs. On a state level, privacy protection may be encompassed within various legal and regulatory frameworks. For more on privacy in the U.S., see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 481 (2006) and see also Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1090 (2002).

[174] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (articulating "the right to be let alone").

[175] *See* Katz v. United States, 389 U.S. 347, 351 (1967) (ruling that warrantless electronic bugging, even when conducted in a public telephone booth, is illegal, and establishing the reasonable expectation of privacy test); *see also* U.S. CONST. amend. IV; Berger v. New York, 388 U.S. 41, 56-57 (1967) (striking down portions of a New York state wiretapping statute because it lacked sufficient judicial review and noting that the Fourth Amendment required "precise and discriminate" limits on its use).

[176] *See* Andrew Crocker, *What to Do About Lawless Government Hacking and the Weakening of Digital Security*, ELEC. FRONTIER FOUND. (Aug. 1, 2016) [hereinafter Crocker, *What to Do About Lawless Government Hacking*], https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security#Title-III [https://perma.cc/UMB4-EB29].

[177] U.N. Report, *supra* note 10, at 4; Ghappour, *supra* note 23, at 1130.

[178] *See* Silverman v. United States, 365 U.S. 505, 511 (1961) (holding that the Fourth Amendment grants a right "to retreat into his own home and there be free from unreasonable governmental intrusion").

Police hacking affects much more than privacy. Wearing a device that shows past and present affects many democratic values and civil rights and liberties such as freedom of speech, association, and movement.[179] Access to one's private communication could also impact their right to religious freedom,[180] as it could reveal their political and religious views and beliefs.[181] It could affect the freedom of the press, as journalists fear governmental surveillance (including revealing their sources).[182] It might violate the rights to due process and fair trial.[183] And it might generally affect the mental health of those spied on.[184]

It could also affect human rights and liberties outside the U.S., as such tools, along with their normalization, might make authoritarian regimes even more oppressive.[185] It could become a highly intrusive oppressive tool for governments to use, which could lead to the arrest, detention, torture and even death of those who were spied on directly or indirectly.[186] And much like the mentioned fears in non-democracies, it might dramatically undermine media freedom everywhere.[187]

And aside from human rights and liberties, which are often the focus of an analysis of this sort, there could be many associated externalities with police hacking, which must be accounted for. One externality is evidence. When granted access to a device, such malware could taint evidence and make it inadmissible in courts.[188] But it could also be used

[179] *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 436-37 (2008) (discussing human rights implications of data mining).

[180] *See* U.S. CONST. amend. I.

[181] *See* U.N. Report, *supra* note 10, at 4.

[182] And it was already proven to be used for illegitimate reasons like against those who express dissenting views like journalists, opposition political figures, and human rights defenders. *See id.* at 2 ("At least 189 journalists, 85 human rights defenders, over 600 politicians and government officials, including cabinet ministers, and diplomats were affected as targets. Investigations also exposed spying on judges, lawyers, doctors, union leaders and academics.").

[183] *Id.* at 4.

[184] *Id.*

[185] *See* Kirchgaessner et al., *supra* note 10.

[186] *See* U.N. Report, *supra* note 10, at 4.

[187] *Id.*

[188] *See* JOHN SCOTT-RAILTON, ELIES CAMPO, BILL MARCZAK, BAHR ABDUL RAZZAK, SIENA ANSTIS, GÖZDE BÖCÜ, SALVATORE SOLIMANO & RON DEIBERT, CATALANGATE: EXTENSIVE

to manipulate data by deleting or adding files (or even communicating with others),[189] and perhaps used to plant evidence and incriminate or blackmail others.[190]

This is essential for the discussion considering another externality — using such an intrusive tool to discriminate against those already over-policed, often due to their race.[191] This fear is non-trivial, as new technologies are often prone to become tools of oppression.[192] Criminal enforcement is often prone to target communities of color, and along with various unlawful misconduct, racial disparities in policing have been statistically proven in many police practices.[193] The use of spyware could likely increase the mistreatment of marginalized communities while legitimizing legal action against them.[194] Police officers might be biased to use such malware against minorities and other over-policed cohorts, thus further perpetuating racial bias and injustice and increasing social control over these communities.[195] This externality is especially crucial everywhere, not only in authoritarian regimes.

Another externality is international in scope. As mentioned, the use of spyware might impact a state's sovereignty. It could thus impact

MERCENARY SPYWARE OPERATION AGAINST CATALANS USING PEGASUS AND CANDIRU 25 (2022), https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru [https://perma.cc/3WK4-D8RF] ("Spyware such as Pegasus modifies the operating system and files on an infected device. It is common guidance that once a device has been remotely penetrated and infected, the integrity of data on the device may be tainted and could certainly be challenged in court.").

[189] *See* U.N. Report, *supra* note 10, at 4.

[190] *Id.*; *see* Niha Masih & Joanna Slater, *Further Evidence in Case Against Indian Activists Accused of Terrorism Was Planted, New Report Says*, WASH. POST (Apr. 20, 2021, 11:30 PM EDT), https://www.washingtonpost.com/world/2021/04/20/india-bhima-koregaon-activists-report [https://perma.cc/6A3H-E29Y].

[191] *See, e.g.*, Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 333, 333 (1998) ("In America, police targeting of black people for excessive and disproportionate search and seizure is a practice older than the Republic itself.").

[192] For the interplay between technology and race, see generally CLARE GARVIE, ALVARO M. BEDOYA, & JONATHAN FRANKLE, THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (2016); Eldar Haber, *Racial Recognition*, 43 CARDOZO L. REV. 71 (2021) [hereinafter *Racial Recognition*].

[193] *See* Haber, *Racial Recognition*, *supra* note 192, at 73.

[194] *Id.*

[195] *Id.*

international relations and lead to foreign relations risks.[196] It could violate the prohibition on the extraterritorial exercise of law enforcement functions without consent under international law.[197] It could even lead to criminal prosecution against police officers and other officials.[198]

The final example of such externalities is security. Police hacking and its use of malware are generally bad for the security of everyone. Keeping known vulnerabilities open could lead to harm.[199] Not disclosing them impacts security.[200] This is especially true for zero-day exploits, which pose a real threat on the one hand but grant access to the police on the other.[201] Thus, when police forces use spyware, they effectively weaken the security of all users, making them more prone to criminal conduct and other potential harm.

[196] *See* Ghappour, *supra* note 23, at 1108.

[197] *Id.* at 1117-18 (making this argument). *But see* Kerr & Murphy, *supra* note 53, at 66 (skeptical of Ghappour's argument).

[198] *See* Ghappour, *supra* note 23, at 1108-22.

[199] *See* U.N. Report, *supra* note 10, at 4; Crocker, *What to Do About Lawless Government Hacking*, *supra* note 176 ("When a government takes a step to create, acquire, stockpile or exploit weaknesses in digital security, it risks making us all less safe by failing to bolster that security.").

[200] *See* Bankston, *supra* note 149. For more on the tension between lawful hacking and security in this context, see Liguori, *supra* note 23, at 334-36.

[201] While there is much secrecy and controversy over whether the government should disclose a zero-day exploit as to patch it, a FOIA suit by the EFF once discovered that at least in 2016, there was an internal policy within the U.S. government's on how to decide whether to retain or disclose a zero day (titled "Vulnerabilities Equities Process."). *See* Crocker, *What to Do About Lawless Government Hacking*, *supra* note 176. Suggested in 2017, the bipartisan Protecting Our Ability to Counter Hacking ("PATCH") Act was aimed to create a "Vulnerability Equities Review Board" that operates independently. Its purpose is to thoroughly assess all software and hardware vulnerabilities in the possession of the federal government, and to disclose the majority of them to the public. *See* PATCH Act, H.R. 2481, 115 Cong. (2017). In some cases, like Operation Torpedo, the government disclosed details on its technique. *See, e.g.*, Joseph Cox, *Judge Rules FBI Must Reveal Malware It Used to Hack Over 1,000 Computers*, VICE (Feb. 18, 2016, 10:02 PM), https://www.vice.com/en/article/jpgmdg/judge-rules-fbi-must-reveal-malware-used-to-hack-over-1000-computers-playpen-jay-michaud [perma.cc/LB3X-9RZB] (discussing a judge's decision for the FBI to reveal the hacking code used in a child pornography case, emphasizing the defense's pursuit for fair trial and broader legal and ethical implications surrounding the case).

All in all, police hacking could be more challenging to regulate than previous technologies like wiretapping and access to stored communication. This mosaic of human rights violations and other potential externalities makes using such an intrusive tool somewhat controversial for the state outside the realm of the Dark Web. At the same time, much like serious offenses on the Dark Web, simply ignoring the technological progress in investigation seems naïve. Police hacking should be permitted in some instances, limited in its applicability, and with effective oversight over its execution. The next Section suggests how.

B. Hold Your Trojan Horses

A balance must be stuck. The police should be able to use malware in some instances and be barred from doing so in others. To delineate such a thick line, policymakers must assess the various impacts of police hacking as shown in Part II.A, and only upon such evaluation can they begin regulating the use of malware under a new legal framework. For now, police hacking outside the realm of the Dark Web must be stopped. The world of externalities and the negative impact on human rights and liberties are not well-assessed yet, and the current legal framework does not consider them properly in light of technology.

Why is the Dark Web excluded from such a moratorium on use? Not because of its bad reputation for being a playground for criminal activities. The Dark Web is also proven to be a "lifeline for those trying to bypass censorship,"[202] especially in authoritarian regimes where access to the internet is curtailed, and thus is essential not to over-police as well, if possible at all. But the way police hacking works in the Dark Web makes a huge difference in balancing enforcement needs and the negative impacts on individuals and society. First, when using malware in Dark Web investigations, the focus is not on spying on individuals but on identifying them after an offense occurs. The malware often generates geographical indications of such culprits, but then the police

[202] Alex Hern, *The Dilemma of the Dark Web: Protecting Neo-Nazis and Dissidents Alike*, GUARDIAN (Aug. 23, 2017, 2:00 PM EDT), https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings [perma.cc/5Q7C-HD46].

resorts to traditional enforcement measures. Second, such use is often against those who engage in serious criminal activities like child pornography, which are crucial to fight against.[203]

It is not that serious crimes do not exist in the physical world or are less important to fight against. And as this Article argues, police hacking should eventually be permitted outside the Dark Web, at least in some contexts. But the difference in the types of data that are revealed, and the fact that spyware is often used to identify culprits upon the commission of a crime, makes a huge difference.

Now for "regular" police hacking, i.e., deploying malware outside the Dark Web. New technological tools like Pegasus, which offer a zero-click attack, are too risky to be used by the police without further inquiry into their negative impact. The Fourth Amendment and even Wiretap's "super-warrant" requirements are not adequately tailored for such use.[204] That is why Congress must first place a mortarium on police hacking outside the Dark Web before police forces in the U.S. follow the Israeli path. Upon placing such a ban, the state should promote further research on how to safeguard the rights of individuals within the use of malware, including how to increase transparency and accountability and provide remedies for those who have suffered harm.[205]

But this ban will be temporary. One can ban companies like NSO from merely creating cyber-attack weapons or place limitations on the import of such tools, but it will primarily have a domestic impact. Banning such use might also lead to spyware emerging illegally which could be under

[203] For more on the importance of fighting against child pornography, see generally Carissa Byrne Hessick, *Disentangling Child Pornography from Child Sex Abuse*, 88 WASH. U. L. REV. 853 (2011).

[204] Notably, many scholars have pointed out the need for reconsidering the scope of the Fourth Amendment in light of new digital technologies. These articles are but mere examples: Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: the Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1094 (1996); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity*, 82 TEX. L. REV. 1349, 1363 (2004); Raymond Shih Ray Ku, *The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1343 (2002); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002). For more on the inapplicability of super-warrants to IoT devices, see generally Haber, *Wiretapping of Things*, *supra* note 26.

[205] *See* Quintin, *supra* note 85.

the radar. In addition, simply blacklisting companies is problematic, as the U.S. might need these companies for its use, even if only for national security and the Dark Web. It is unclear why the FBI decided not to use Pegasus, a highly sophisticated hacking tool. Perhaps it is too expansive for the state.[206] Perhaps they do not want a foreign company to thrive and potentially spy on them as well. And perhaps the fact that police hacking is resource-intensive and depends on having a suspect with a specific vulnerability, might lead the state to pursue other investigative means.[207]

It seems unlikely that the state will not use the market.[208] With all the capabilities of the state, enforcement agencies are highly reliant on the market to decrypt technology or deploy malware.[209] It was a private company that aided the FBI in unlocking the San Bernardino iPhone.[210] Companies like NSO provide law enforcement agencies worldwide with hacking malware like Pegasus to aid, at least declaratively, against terror and serious crimes.[211] They can place bans on specific companies like NSO, but they will likely continue relying on them. Not only because the

[206] These tools might be costly; at least in 2016, the New York Times argued that using NSO's spyware will cost "$650,000, plus a $500,000 setup fee with an Israeli outfit called the NSO Group." Perlroth, *supra* note 49; *see also* Liguori, *supra* note 23, at 333 ("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.").

[207] *See* Bankston, *supra* note 149.

[208] Let us assume that Pegasus and its like are banned. Private companies cannot engage in such practices at all. Unless the government develops such capabilities, it will not be able to use such technology. It is hard to evaluate if the cyber "black" market can provide similar tools to Pegasus. Still, it should be noted that these are highly sophisticated viruses that cost millions of dollars to develop and have a relatively short shelf life, as once detected, the operating system will likely be updated to eliminate the vulnerability. *See* Priest, Timberg & Mekhennet, *supra* note 75 (quoting Ivan Krstić, head of Apple Security Engineering and Architecture, stating "[a]ttacks like the ones described [NSO's] are highly sophisticated, cost millions of dollars to develop, often have a short shelf life and are used to target specific individuals.").

[209] *See* Kerr & Schneier, *supra* note 39, at 1012 ("Expertise relevant to workarounds will be found outside the government.").

[210] *See* Ellen Nakashima & Reed Albergotti, *The FBI Wanted to Unlock the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm.*, WASH. POST (Apr. 14, 2021, 8:00 AM EDT), https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi [perma.cc/BTM8-VQWU].

[211] *See* Perlroth, *supra* note 49.

state is more limited than private companies in developing these tools but also because police hacking is proven as an essential tool in some criminal cases. The efficiency of such practice, along with its relative success, is likely to continue it. With malware, the state no longer relies on digital intermediaries' willingness to cooperate,[212] and even on other states.[213] It saves precious time, which in the criminal investigation might be crucial, and can almost immediately connect directly to a suspect.[214]

Thus, upon placing such a moratorium, policymakers should consider how to regulate police hacking properly. Unlike in the Israeli revelations, where it is still controversial whether such malware should be permitted under the law,[215] U.S. law must distinguish between stored communication, wiretaps, and lawful hacking.[216] They must construct a new judicial paradigm. And such a paradigm does not begin from scratch. As others have suggested, the state should only employ spyware as a last resort where less pervasive means of investigation have failed; it must be made only upon mandatory judicial authorization; it should be limited in duration and scope; and it should only be used for severe crimes investigations.[217] Policymakers must also strive to educate judges

[212] These private companies might not only be reluctant to aid the police, but also might deliberately not save the data of their users, or even not have direct access to their communication. *See* PRIV. INT'L, GOVERNMENT HACKING AND SURVEILLANCE: 10 NECESSARY SAFEGUARDS 7 (2018), https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf [perma.cc/R8M3-DJHQ].

[213] *Id.*

[214] *Id.* ("Governments have therefore typically relied on the cooperation of a third party — a company, foreign government, or even both — to access this data. This process is typically time-consuming and may prove fruitless if the company or foreign government is unwilling or unable to provide access. Hacking can therefore be more convenient than legal processes involving multiple parties.").

[215] *See* Bergman & Mazzetti, *supra* note 76.

[216] Currently, as Part I.B showed, malware is governed by the Fourth Amendment, Rule 41, and the ECPA. Depending on the use of the malware, the government will need to obtain some type of legal authorization, which at most will be equivalent to a wiretap super-warrant.

[217] *See, e.g.*, Liguori, *supra* note 23, at 332 (arguing that lawful hacking techniques should be employed only as an *ultima ratio*). The definition of "serious" or "severe" crimes could significantly differ between states. To exemplify, while in the U.S. such crimes might be those punishable by imprisonment for more than one year (felonies), serious crimes in Israel are defined as any offense for which "the national law imposes a

technically and normatively about malware, its delivery and execution, and its consequences.[218]

These suggestions should serve as a baseline for discussion. The use of malware must be well-defined under the statute.[219] Such use must be restricted only for the harshest of offenses and a last resort where less pervasive means of investigation have failed.[220] At this point, it is crucial first to evaluate the purpose of using such malware. If it is used for identification purposes, judges must make sure that the malware in question is constructed in such a way that only allows the functionality related to identifications. That means that the malware could only be executed technologically under the court's order.[221] That means the time they can use the malware, what they can do with it, and which data and metadata they can obtain. These wiretaps could be almost entirely digital, thus creating oversight by design.

But before issuing such a warrant, the court must assess the gravity of the offense. Malware is not a replacement for wiretaps or searching stored communication. It should not be granted for every felony, only those society deems most crucial for public safety. It should also be reserved for instances in which either investigation took time, and due to the nature of the crime, it is crucial to identify the culprit. It could also be used where time is of the essence, like in kidnapping, aside from terrorism.[222] The state must demonstrate to the court that malware is

term of imprisonment of 6 years or more." Judah Ari Gross, *Amid Fallout from NSO Scandal, Israel Imposes New Restrictions on Cyber Exports*, TIMES OF ISRAEL (Dec. 6, 2021, 8:22 PM), https://www.timesofisrael.com/amid-fallout-from-nso-scandal-israel-imposes-new-restrictions-on-cyber-exports [perma.cc/Y3FC-8VSR].

[218] *See, e.g.*, Liguori, *supra* note 23, at 332 (arguing that educating judges on the technical nuances and potential consequences of lawful hacking presents a distinct challenge).

[219] *See* Crocker, *What to Do About Lawless Government Hacking*, *supra* note 176 (suggesting that it is better to have affirmative rules).

[220] *See* PRIV. INT'L, *supra* note 212, at 11-12.

[221] That is unlike how the FBI often asked the court "to trust that it would operate its malware safely." Crocker, *What to Do About Lawless Government Hacking*, *supra* note 176.

[222] *See* U.N. Report, *supra* note 10, at 5 ("Even if legitimate goals are being pursued, such as national security objectives or the protection of the rights of others, the assessment of the necessity and proportionality of the use of spyware severely limits the scenarios in which spyware would be permissible.").

the least intrusive option and only used as a last resort.[223] The state must disclose the method used, at least in general terms, and confine the use both in scope and at the time of the hack.[224]

These warrants should have steps. It should not be a binary decision of using malware, but rather one that is tailored specifically for each case. The government must convince the court why such malware is needed. It must evaluate and demonstrate the risks to the target and other systems, data, and ways to mitigate damage.[225] The government must show a high probability of a serious crime and that hacking is the only way to obtain evidence. The evidence must be relevant to the case and stored in the suspect's system.[226] Only relevant and material data on the alleged serious crime will be accessed and collected.[227]

The duration must be shorter than regular wiretaps. It should be for minutes, maybe seconds. It must not become a fishing expedition for new evidence, but mainly as a tool for identifying or locating suspects, much like within the Dark Web. The government can only modify data as necessary for authorized hacking and must keep a record of all activities. If data obtained through hacking is used, the government must disclose its methods and records to the target person.[228] Any irrelevant or immaterial data obtained through authorized hacking must be promptly destroyed, and the destruction must be recorded in the audit trail of hacking activities.[229]

When used, and depending on the purpose of such use, the malware will first only allow the elements necessary for identification, like geolocation. If such metadata does not aid, the malware can allow other functions, like taking a quick photo of the suspect or opening the microphone for a short while. If that does not help the investigators, the malware can access some stored communication like email to find out

[223] *See id.* at 6 ("This should be a last resort, in other words, all less intrusive measures should have been exhausted or have been shown to be futile, and should be strictly limited in scope and duration."); PRIV. INT'L, *supra* note 212, at 12.

[224] *See* PRIV. INT'L, *supra* note 212, at 12.

[225] *See id.* at 11.

[226] *See id.* at 11-12.

[227] *See id.* at 12.

[228] *See id.* at 13-14.

[229] *Id.*

the identity of the culprit, if it is unknown, or other stored communication relevant to the warrant's specific purposes. The state must resort to more "traditional" methods upon exhausting all such moves. Then, the specific malware must become non-operational for future use.

This is a blueprint for legalizing police hacking. Such hacking can only occur under a rigorous legal framework that governs its use along with rigorous external oversight.[230] When judges consider granting access to a suspect's computer, they must consider the potential implications of such a warrant on the security of the device in question, the security of other related systems or individuals, the privacy implications for all involved, and all other related externalities.[231]

At the same time, increasing transparency and oversight over such a process is crucial. We must have transparency over the use of such warrants, both technologically (as described) and physically. Such transparency is not necessarily an absolute one. While the police must reveal to the court which functions of the malware they will use (e.g., microphone, video, or text), the exact type of malware is less relevant and should remain in the dark. Such malware will be configured to the warrant requirements anyhow. But to decide which malware to use, the police must be able to work with any vendor in the industry, as they are unlikely to produce sophisticated tools for all devices by themselves.

Police oversight is the most crucial element here. The government must be able to assess how the police work in real time. The state needs more expertise within courts, at least in areas of a fast-paced evolution like technology. Computer scientists that can examine the malware and the exploit, along with legal experts in the field of law and technology that can examine the meaning of such malware and exploit, should aid judges in creating guidelines when authorizing warrants. The meaning of such "search" requires technological expertise.[232] They should also

[230] *See* U.N. Report, *supra* note 10, at 6 ("The measures should also be subject to rigorous independent oversight; prior approval by a judicial body is essential.").

[231] *See* PRIV. INT'L, *supra* note 212, at 11.

[232] For more on the need for expertise in using malware, see generally Rupinder K. Garcha, *NITS a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases*, 93 N.Y.U. L. REV. 822 (2018) and Schwartz, *supra* note 36, at 1699 ("Different

evaluate the consequences of the search both domestically and internationally.[233]

The state must thus work with data scientists and other experts to make sure that: (1) evidence is not tainted; (2) there is no incrimination; (3) oversee that the warrant is correctly hard-coded into the malware; (4) oversee the police use of such malware as to reevaluate its potential impact on human rights and liberties, its necessity in aiding public safety, and to make sure the police does not use such malware unfairly or otherwise discriminatorily. Such oversight must be done in real time, not only ex-post. An oversight body must also make sure that the software is not threatening democracy, e.g., not used as a tool for the persecution of political dissidents.[234] Congress must also oblige effective reporting on the general use of such warrants and their issuing,[235] including statistics on suspects to examine misuse against some cohorts. Courts must publish the number of hacking applications approved and denied, the government authorities that applied, the offenses specified, and the details of authorized hacking measures, including target system configurations.[236] It would be unfortunate to have another Snowden moment, equivalent to the Israeli revelations on NSO.

Regulating the use of police hacking should also exceed the state's borders. This realm cannot be left without meaningful international intervention. States worldwide must strive to set intentional rules and

clouds lead to different answers to questions about ability to access data and the location of data.").

[233] This could be important with searching the cloud. As previously mentioned, such a search could occur in multiple international locations, when each file might "be broken into components and stored in different countries" and might also be constantly in motion. *See* Schwartz, *supra* note 36, at 1695.

[234] *See* Stephanie Kirchgaessner & Sam Jones, *Phone of Top Catalan Politician "Targeted By Government-grade Spyware*," GUARDIAN (July 13, 2020, 6:15 PM EDT), https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware [perma.cc/LFX2-MG55].

[235] *See* Crocker, *What to Do About Lawless Government Hacking*, *supra* note 176 (suggesting public reporting requirements).

[236] *See* PRIV. INT'L, *supra* note 212, at 13-14.

standards, not generally as cybercrime[237] or under limited agreements on dual-use technologies,[238] but more globally and directly. Such agreements will oblige other states to control the use of sophisticated weapons like Pegasus, especially when they might end up in authoritarian regimes. It will also set an international threshold on the restrictions for using police hacking while limiting their ability to export such dual-use weapons to regimes that disregard such a minimal threshold. There must be clear lines between serious crimes and others, regardless of a specific regime.[239] Non-democratic societies cannot rely on the market in democracies. It is not enough that these states or private mercenaries declare that it is only used for kidnappers and drug lords; aside from terrorists, it must be set by law.[240]

States will also have to keep a close eye on the use of such spyware internationally, aside from state espionage or military operations. States might use this much like any other weapon they give to other countries to fulfill their domestic interests, much like they do in proxy wars.[241]

[237] While the cyber field is largely unregulated within the international sphere, some agreements or conventions exist. Mainly, perhaps is the Council of Europe's Convention on Cybercrime (known as the Budapest Convention), which, in the context of this Article, does not authorize remote cross-border searches. *See* Convention on Cybercrime, art. 32, *opened for signature* Nov. 23, 2004, S. Treaty Doc. No. 108-11, 2296 U.N.T.S. 167 (entered into force July 1, 2004). The U.S. Senate ratified it in September 2006. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUR., https://go.coe.int/Be71y (last visited Sept. 22, 2023) [perma.cc/JUX8-YKEC].

[238] The reference is to the Wassenaar agreement which sets a multilateral export control regime. It aims to prevent the accumulation of conventional arms and dual-use goods and technologies that may threaten regional and international security, which could include the use of spyware. *See What is the Wassenaar Arrangement?*, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/the-wassenaar-arrangement (last visited Sept. 22, 2023) [perma.cc/G6AN-GGT7].

[239] In Israel, for instance, upon one of the intentional controversies of using NSO's spyware worldwide, the Defense Ministry's Defense Export Control Agency, updated its forms that are required for selling cyber-related products abroad, while explicitly stating that "an act of expressing an opinion or criticism" does not constitute a "Terrorist Act" or a "Serious Crime." Gross, *supra* note 217.

[240] *See* Perlroth, *supra* note 49 ("The industry argues that this spying is necessary to track terrorists, kidnappers and drug lords.").

[241] The CIA, for instance, was reported to purchase Pegasus for Djibouti in their combat against terrorism. *See* Farrow, *supra* note 86. A spokesman for the government of Djibouti government denied any use of Pegasus. Bergman & Mazzetti, *supra* note 76.

While it is difficult to achieve consensus, states must strive to more attentively use such spyware.[242] It might be wise to place a mortarium on international use until states regulate it domestically.[243] Like any other weapon, controlling the export of malware could be highly beneficial for countries.[244] Such decisions could tilt who wins a war or strengthen countries' ability domestically and internationally. And countries that have such control could also benefit in other areas.[245]

Essentially, Congress will have to make an official stand. It must regulate hacking much as it did for wiretapping, which took seventy-eight years to do so.[246] And since hacking is more intrusive to civil rights and liberties, and creates more externalities, let us hope it will take less time. Such a move is vital to grant certainty of what the government can and cannot do with spyware.[247] Failing to act might make police hacking legitimized and then normalized. When the FBI publicizes that it uses spyware (or, in its words, "NITs") to fight against child pornography,[248] and companies like NSO declare that "[p]edophiles and terrorists can freely operate in technological safe-havens, and we provide governments the lawful tools to fight it,"[249] it is not likely to attract any public outcry. And when such use is within the so-called "Dark Web," people will likely approve of such practices more

[242] *See* Ghappour, *supra* note 23, at 1119-21.

[243] *See* Tom Miles, *U.N. Surveillance Expert Urges Global Moratorium on Sale of Spyware*, REUTERS (June 18, 2019), https://www.reuters.com/article/us-socialmedia-un-spyware/u-n-surveillance-expert-urges-global-moratorium-on-sale-of-spyware-idUSKCN1TJ2DV [perma.cc/TS9F-XB9W] ("The world should impose a moratorium on the sale and use of surveillance software until there are rules in place to stop governments using it to spy on opponents and critics . . . .").

[244] *See* Bergman & Mazzetti, *supra* note 76.

[245] Israel's control over NSO's cyberweapons was suggested to tilt Mexico and Panama's position toward Israel within the international arena like the United Nations and might have played a role in support of Arab nations against Iran and in negotiating the Abraham Accords, which normalized relations between Israel and several Arab nations. *See id.*

[246] While wiretapping is known to exist at least since 1890, and aside from an act that slightly began its regulation, wiretapping was only effectively regulated in 1968. *See* Haber, *Wiretapping of Things*, *supra* note 26, at 738-40.

[247] *See* Bankston, *supra* note 149.

[248] *See* Poulsen, *supra* note 56.

[249] Perlroth, *Apple Sues Israeli Spyware Maker*, *supra* note 159.

generally without realizing their destructive nature and externalities. The fear here is that such publicity casts a smoke screen on police hacking in other criminal activities that are highly remote from child pornography and the use of anonymized networks. One can only hope the Israeli revelations have little to do with police hacking in the U.S. But even if so, it is crucial to set the legal playing field for a practice that will not likely cease anytime soon.

Conclusion

Technology and criminal investigation will keep playing a cat-and-mouse game. While police hacking is nothing new, and we have known about this practice for a long time, the Israeli revelations about governmental use of NSO's Pegasus spyware might aid in unveiling similar practices worldwide. And even if Israel is unique in the democratic-states view, the U.S. must stop turning away from the pressing issue of regulating spyware use in the hands of law enforcement. The Israeli revelations should at least spark a worldwide discussion on the necessity for a new legal framework that will significantly limit the ways police hacking occurs and, perhaps more importantly, ensures that such practice is appropriately governed and not commenced outside public scrutiny.

New technologies may make police hacking obsolete soon. With the advancement of new technologies that promise virtual spaces where we might shift our lives, perhaps the future of criminal enforcement will significantly change in the upcoming years. But currently, at least, the use of spyware is only likely to continue with the increased use of connected devices, and police forces around the globe will not likely forsake such tools. This is where the suggested blueprint should come in handy for policymakers in the U.S. and elsewhere. But Congress must first place a mortarium on most forms of police hacking until such a new enforcement method is appropriately legalized.