ARTICLES

THE PEGASUS ERA: REGULATING A NEW GENERATION OF GOVERNMENT SPYWARE

YOTAM BERGER*

ABSTRACT

The exposure of Pegasus, a spyware developed by the Israeli company NSO Group, marked a new era in cybersurveillance. Capable of remote, zero-click infiltration of mobile devices, Pegasus grants operators near-total control over a device for surveillance purposes. Although marketed as a tool for combating terrorism and crime, it has also been widely abused to target journalists, human rights activists, and leaders of political opposition.

This Article examines the legal and regulatory challenges posed by tools like Pegasus, focusing on their potential use by law enforcement agencies in democratic societies, particularly the United States. Building on comparative experiences from Israel and the European Union, the Article highlights how different jurisdictions have grappled with similar challenges, offering lessons for U.S. policymakers.

The Article presents three key arguments. First, these tools should be treated as a diverse "toolbox," rather than a single unified tool. Different features require distinct legal frameworks and strict limitations tailored to specific legal contexts, as evidenced by a comparative analysis. Second, in the U.S. context, the act of infecting a device must be recognized as the initiation of a search under the Fourth Amendment, necessitating appropriate judicial oversight from the moment of infection. Third, while certain capabilities of these tools align with existing U.S. legal doctrines, new legislation is essential to address the broader implications of the Pegasus Era. Together, these findings highlight the need for proactive reforms to balance the enhanced capabilities of law enforcement with the protection of constitutional rights and individual privacy.

---

* JSD Candidate, Stanford Law School. I would like to thank Michael Birnhack, Ilana Felsenthal, George Fisher, Bruria Friedman-Feldman, Orin Kerr, Amalia Kessler, Claire Lazar-Reich, Tom Nachtigal, Richard Salgado, Shirin Sinnar, David Sklansky, Allen Weiner, Stanford's Gordian Knot Center for National Security Innovation, Knight-Henessy Scholars, the Stanford Interdisciplinary Graduate Fellowship, and the editorial board of the Georgetown Journal of International Law for their support, guidance, and helpful comments. Opinions and mistakes are, of course, my own.

I. Introduction

July 18, 2021, marks a pivotal moment in the current age of cybersurveillance, in which anyone's phone can become a spy in their pocket. On that day, the Pegasus Project—a collaboration of journalists from eighteen news organizations—unveiled its investigation into Pegasus, a spyware developed by the Israeli company NSO Group and deployed by governments around the world.[1] The investigation revealed Pegasus to be not only extraordinarily intrusive but also highly prone to abuse in the wrong hands. This software could infiltrate a phone remotely, without the user's consent or even their awareness.[2] Once installed, Pegasus gained access to nearly all of the phone's features, allowing it to view stored data, monitor new content in real-time, and even activate the device's microphone and camera to record its surroundings.[3] This could often be done on a zero-click basis, meaning the user did not even need to click a malicious link for their device to be compromised.[4] The capabilities of Pegasus were shocking enough themselves, but the list of targets, ranging from heads of state and opposition leaders to journalists and human rights activists, was particularly alarming.[5]

Pegasus was marketed by NSO as a legitimate law enforcement tool; to this day, the company claims it to be an effective tool to combat terrorism, drug cartels, and pedophiles.[6] The Pegasus Project focused mostly on what happened when this tool was abused, typically by authoritarian regimes, to oppress opposition leaders and civil society. But according to the reports, among this tool's clients were many democratic countries too, including the United States.[7] Further, NSO's product is just one among many available to law enforcement agencies and state actors in the market today. What happens when democracies use these tools for their allegedly legitimate law enforcement ends? Should such practices be allowed? Are they allowed today in the United States, and if so, who regulates them? How do existing U.S. legal doctrines

1. *About the Pegasus Project*, Forbidden Stories (July 18, 2021), www.forbiddenstories.org/about-the-pegasus-project/.

2. David Pegg & Sam Cutler, *What is Pegasus spyware and how does it hack phones?*, The Guardian (July 18, 2021), www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

3. *Id.*

4. *Id.*

5. Craig Timberg et al., *On the list: Ten prime ministers, three presidents and a king*, Wash. Post (July 20, 2021), www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware.

6. *About us*, NSO Group, (last visited Nov. 21, 2024), www.nsogroup.com/about-us/.

7. Stephanie Kirchgaessner, *FBI confirms it obtained NSO's Pegasus spyware*, The Guardian (Feb. 2, 2022), www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware.

apply to the availability of these tools, and how should they be reviewed to ensure public safety and protect constitutional rights? Can the United States draw conclusions from previous experiences of other democratic societies in this context? This Article is a starting point for examining these questions.

The Article begins in Part II by describing what we know about this new age of cybersurveillance. It first introduces Pegasus and summarizes publicly available information about other companies in the field that apparently offer similar products. It further reviews what these programs can do. The Article then argues that commercial spyware could be legitimately used in democratic societies, including the United States. However, the situations in which law enforcement agencies should be allowed to use these toolboxes must be strictly defined in advance and closely regulated.

Building on that background, Part III examines the comparative experiences of other democratic societies. It focuses on the Merari Report issued by the Israeli Ministry of Justice and the PEGA Report of the European Union (EU or the Union). It highlights key lessons that U.S. stakeholders can draw from the challenges these nations encountered during the Pegasus crisis and their subsequent responses.

Parts IV and V then dive into U.S. law, providing frameworks for examining how these programs may be operated and regulated in the United States. Part IV focuses on the intersection of commercial spyware use and the Fourth Amendment. It argues that despite some legal and interpretational challenges, using spyware in law enforcement must be understood as a "search" under the Fourth Amendment. Further, this part explores at what point a warrant should be obtained and argues that a "search" using the tools begins at the moment of infection, not at the moment of the actual review of content accessible through an infected device. Part V explores the intersection of different capabilities these tools present with existing U.S. statutory frameworks. It argues that some of the abilities of these tools are merely advanced versions of existing practices, such as wiretapping, and could be covered by existing legislation. Other capabilities, however, are fundamentally different and should be addressed by new legislative frameworks.

In other words, this Article warns that the United States, like other democratic nations, is entering a new age of cybersurveillance: the Pegasus Era. In this era, practically anyone who owns a phone could find their device infected with software that transforms it into an extraordinarily powerful surveillance tool capable of exposing the most intimate details of their life. While these tools hold great potential for more effective law enforcement, they also present serious risks to

human rights and freedoms. This Article examines the legal ramifications of this new era in democratic societies and explores the emerging, as well as future, challenges it will create for law enforcement and courts in the United States, urging a proactive approach to address these challenges.

II. A New Age of Cybersurveillance

The revelations about Pegasus's operations have brought significant public attention to the cybersurveillance industry. This part examines what is currently known about the industry, focusing on Pegasus. It begins by detailing the brief history of this product, before elaborating on what we know about the technical mechanisms underpinning Pegasus's operation. It then introduces the primary argument for the potentially legitimate use of tools like Pegasus: the "going dark" argument.

A. *Pegasus and the Commercial Spyware Industry*

To this day, NSO's website presents the company as "developing technology to prevent and investigate terror and crime."[8] This statement seems to be the company's main selling point. NSO Group was founded in 2010 by three Israeli citizens: Omri Lavie, Shalev Hulio, and Niv Karmi.[9] Their product, Pegasus, is a program that allows operators to break into mobile devices remotely. It was intended to be purchased by governments seeking to combat crime and terrorism.[10] According to Hulio, the first time the company was contacted by a world leader was in late 2011, when the President of Mexico showed interest in their program to target drug cartels, though he also said they had been contacted by other state actors well before that.[11]

NSO's existence was known well before the Pegasus Project went public. As early as 2009, NSO started as a company named CommuniTake, which originally developed a program that allowed support technicians to take over a customer's phone remotely to fix technical issues, with the

8. NSO Group, *supra* note 6.

9. Gabrielle Coppola, *Israeli Entrepreneurs Play Both Sides of the Cyber Wars*, Bloomberg (Sept. 29, 2014), www.bloomberg.com/news/articles/2014-09-29/israeli-entrepreneurs-play-both-sides-of-the-cyber-wars; Elizabeth Dwoskin & Shira Rubin, *'Somebody has to do the dirty work': NSO founders defend the spyware they built*, Wash. Post (July 21, 2021), www.washingtonpost.com/world/2021/07/21/shalev-hulio-nso-surveillance/.

10. NSO Group, *supra* note 6.

11. *See* Laurent Richard & Sandrine Riguad, Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy 49-50 (2023). *See also* Ronen Bergman, *Weaving a cyber web*, Ynet (Nov. 1, 2019), www.ynetnews.com/articles/0,7340,L-5444998,00.html.

customer's consent.[12] According to their account, the founders later realized that their technology could be used to gather intelligence.[13]

State hacking existed, of course, well before Pegasus.[14] However, its unique intrusiveness, advanced zero-click capabilities, and the technical ability to easily target practically anyone with a phone drew unique public attention to it even before the Pegasus Project unveiled its investigation. In fact, journalists had covered NSO's offensive cyber operations that were sold to state actors years before the publication of the Pegasus Project.[15] For instance, in 2016, human rights lawyer Ahmed Mansoor was reportedly targeted by Pegasus.[16] After receiving a suspicious message with a link promising "secrets" about tortures in the United Arab Emirates, he handed his phone to experts, who warned that NSO had found at least three vulnerabilities that were previously unknown to the security industry.[17] In another example that made the headlines in 2017, the New York Times reported that Pegasus was "oddly" targeting the backers of Mexico's soda tax, a political initiative aimed at reducing the consumption of sugary drinks in the country.[18]

In 2018, Jamal Khashoggi, a Saudi journalist who contributed to various publications, including the Washington Post, was killed at the Saudi consulate in Istanbul.[19] Within a few weeks, the media started reporting claims that the Saudi government used Pegasus to track Khashoggi before his assassination.[20] NSO denied the allegations,[21] but

12. *Id.* at 52.

13. *Id.* at 52-55.

14. *See, e.g.,* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075 (2017); Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web*, 70 STAN. L. REV. 58 (2017).

15. *See, e.g.,* Dave Lee, *Who are the hackers who cracked the iPhone?*, BBC (Aug. 26, 2016), www.bbc.com/news/technology-37192670.

16. *Id.*

17. *See id.* Known as "Zero Day" vulnerabilities, not to be confused with Zero Click vulnerabilities.

18. Nicole Perlroth, *Spyware's Odd Targets: Backers of Mexico's Soda Tax*, N.Y. TIMES (Feb. 11, 2017), www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html.

19. Julian E. Barnes et al., *'Tell Your Boss': Recording Is Seen to Link Saudi Crown Prince More Strongly to Khashoggi Killing*, N.Y. TIMES (Nov. 12, 2018), www.nytimes.com/2018/11/12/world/middleeast/jamal-khashoggi-killing-saudi-arabia.html.

20. *See, e.g.,* Hagar Shezaf, *Snowden: Israeli Firm's Spyware Was Used to Track Khashoggi*, HAARETZ (Nov. 7, 2018), www.haaretz.com/israel-news/2018-11-07/ty-article/.premium/israeli-spyware-was-used-to-track-saudi-journalist-khashoggi-edward-snowden-says/0000017f-e09f-df7c-a5ff-e2ffc1650000.

21. *NSO founder denies its phone hacking software was used to track Khashoggi*, TIMES OF ISR. (Jan. 12, 2019), www.timesofisrael.com/nso-founder-denies-its-cellphone-hacking-software-used-to-track-khashoggi.

the Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, found otherwise. In a report issued in October 2018, researchers at the Citizen Lab detected that Saudi dissident Omar Abdulaziz, who was in touch with Khashoggi before his death, was targeted by an NSO-made program.[22] "The hacking of my phone played a major role in what happened to Jamal," Abdulaziz later told CNN.[23] Nonetheless, NSO insisted that the company is merely the manufacturer of a legitimate law enforcement tool that always ensures public safety and promotes criminal justice when used by state actors, and had nothing to do with the Khashoggi case.[24]

Then came the Pegasus Project. It revealed that NSO sold their powerful spyware to various regimes, some of which are authoritarian. The scoop was based on a document known as "The List"—a file including around 50,000 phone numbers of devices that have been targeted by Pegasus, which was leaked by an unknown source.[25] Among them, the Pegasus Project team identified the phone numbers of dozens of journalists, human rights activists, academics, businesspeople, lawyers, doctors, diplomats, union leaders, and politicians.[26]

The publication of the Pegasus Project revealed in detail what exactly this program does. "Once installed," the French publication that orchestrated the Pegasus Project, Forbidden Stories, reported, "it allows clients to take complete control of the device, including accessing messages from encrypted messaging apps . . . and turning on the microphone and camera."[27] Pegasus can break into a phone remotely, without the user's consent or knowledge,[28] and often works on a zero-click basis.[29] Once a phone is infected, Pegasus gains full access to most of its

22. Bill Marczak et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, CITIZEN LAB (Oct. 1, 2018), www.citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

23. Nina dos Santos & Michael Kaplan, *Jamal Khashoggi's private WhatsApp messages may offer new clues to killing*, CNN (Dec. 4, 2018), www.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html.

24. Patrick Howell O'Neill, *The man who built a spyware empire says it's time to come out of the shadows*, MIT TECH. REV. (Aug. 19, 2020), www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/; Stephanie Kirchgaessner, *Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests*, THE GUARDIAN (Jul. 18, 2021), www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.

25. Pegg & Cutler, *supra* note 2.

26. *See* FORBIDDEN STORIES, *supra* note 1.

27. *Id.*

28. *Id.*

29. Pegg & Cutler, *supra* note 2.

features: it allows the operator to read everything sent through the phone, whether encrypted or not.[30] It also gains full access to the device's camera and microphone, allowing the operator to eavesdrop and film everything, even if the user has not launched the camera.[31]

Over the years, and to this day, NSO insists Pegasus is a legitimate law enforcement tool. NSO's founders said that this was the case even after the Pegasus Project began publishing their stories. In an interview with the Washington Post a few days after Forbidden Stories' initial report on "The List," NSO's CEO, Hulio, denied most of the allegations against the company and claimed their enterprise was well-regulated.[32] "[For] the people that are not criminals, not the Bin Ladens of the world—there's nothing to be afraid of," he told Forbes on July 22, 2021.[33]

The Pegasus Project later focused on debunking these claims. Time and time again, their publications, and other publications that followed, stated that NSO sold their spyware to regimes that abused it. There was worry among many who were not, as Hulio puts it, "the Bin Ladens of the world." The Washington Post named at least ten prime ministers, three presidents, and one king who were targeted by Pegasus in France, Iraq, South Africa, Egypt, Morocco, Pakistan, and more.[34] Over 180 journalists were on "The List,"[35] and so were many civil society and human rights activists.[36]

Indeed, the Pegasus Project focused mostly on authoritarian regimes that accessed the program. But they are certainly not the only governments that bought that specific product or similar products. The FBI, for instance, reportedly gained access to Pegasus.[37] The United States later posed severe restrictions on NSO, yet installed its servers in a facility in New Jersey around 2019.[38] Further, the Israeli police used a

30. RICHARD & RIGAUD, *supra* note 11, at 6.

31. *Id.*

32. Dwoskin & Rubin, *supra* note 9.

33. Thomas Brewster, *'If You're Not A Criminal, Don't Be Afraid'—NSO CEO On 'Insane' Hacking Allegations Facing $1 Billion Spyware Business*, FORBES (July 22, 2021), www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/.

34. Timberg et al., *supra* note 5.

35. Phineas Rueckert, *Pegasus: The new global weapon for silencing journalists*, FORBIDDEN STORIES (July 18, 2021), www.forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

36. Shaun Walker et al., *Pegasus project: spyware leak suggests lawyers and activists at risk across globe*, THE GUARDIAN (July 19, 2021), www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe.

37. Kirchgaessner, *supra* note 7.

38. Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES MAG. (June 15, 2023), www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [hereinafter *Battle for the World's Most Powerful Cyberweapon*].

version of the program.[39] A special committee of inquiry in the Israeli Ministry of Justice even found that most of its use was coherent with Israeli criminal procedure.[40] However, the Israeli prosecution admitted that in at least one murder case, they illegally obtained evidence using spyware, and the evidence was therefore excluded.[41]

NSO had at least twenty-two clients in some fourteen Member States of the EU, too.[42] Perhaps not surprisingly, Poland and Hungary were among NSO's clients.[43] These two are sometimes characterized as countries suffering from democratic backsliding.[44] But other Member States that may be perceived as more committed to human rights and privacy also obtained the program, including Germany.[45] The European Parliament later appointed a special committee to investigate how the program and similar spyware have been used in EU jurisdictions.[46]

---

39. Tomer Ganon, חברת אן.אס.או בשירות משטרת ישראל: פריצות לטלפון של אזרחים ללא פיקוח או בקרה *[NSO in the service of the Israeli police: Broke into Phones of Citizens]*, CALCALIST (Jan. 18, 2022), www.calcalist.co.il/local_news/article/s1b1xwx6y (Isr.) [hereinafter *NSO in the service of the Israeli police*].

40. AMIT MERARI ET AL., MINISTRY OF JUST., דו"ח הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים [Report of the team investigating wiretapping on communications between computers] (2022) (Isr.).

41. Lior El-Hai & Gilad Morag, הפרקליטות משכה ראיות מתיק רצח כפול בגלל שימוש ברוגלות מצד המשטרה [*State Attorney to Give Up on Evidence in a Double Murder Case because the Police Illegally Used Spyware*], YNET (June 5, 2023), www.ynet.co.il/news/article/ry2qfwouh (Isr.).

42. The client list could include different agencies in the same country. Omer Benjakob, *Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It's Not Alone*, HAARETZ (Aug. 9, 2022), www.haaretz.com/israel-news/security-aviation/2022-08-09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000.

43. Wojciech Kość, *Poland launches Pegasus spyware probe*, POLITICO (Feb. 19, 2024), www.politico.eu/article/poland-pegasus-spyware-probe-law-and-justice-pis-jaroslaw-kaczynski/; Jakub Iwaniuk, *Pegasus probe in Poland reveals unprecedented use of spyware by previous government*, LE MONDE (Mar. 4, 2024), www.lemonde.fr/en/international/article/2024/03/04/pegasus-probe-in-poland-reveals-unprecedented-use-of-spyware-by-previous-government_6584086_4.html; Justin Spike, *Hungarian Official: Government Bought, used Pegasus Spyware*, ASSOCIATED PRESS (Nov. 4, 2021, 1:05 PM), www.apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0.

44. *See, e.g.*, Michael Bernhard, *Democratic Backsliding in Poland and Hungary*, 80 SLAVIC REV., 585 (2021).

45. Shira Silkoff, *German federal police acquired Pegasus spyware in secret*, JERUSALEM POST (Sep. 8, 2021), www.jpost.com/international/german-federal-police-acquired-pegasus-spyware-in-secret-678921; AFP Staff, *Germany admits police used spyware from NSO Group in 'small number of cases'*, TIMES OF ISR. (Sept. 7, 2021), www.timesofisrael.com/germany-admits-police-used-spyware-from-nso-group-in-small-number-of-cases/.

46. Costica Dumbrava, *Investigation of the use of Pegasus and equivalent surveillance spyware*, EUR. PARL. RSCH. SERV. (Jun. 2023), www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf.

According to the report, such programs were used by many other Member States, including for example Spain and the Netherlands.[47]

Mexico was among NSO's clients as well. Indeed, according to the Pegasus Project, the spyware was abused in the country, for instance, by targeting reporters and legitimate political activists.[48] Alternatively, it was used to fight drug cartels and may have enabled the prosecution of a prominent cartel leader.[49]

NSO's business was seriously damaged by the publications of its activities. Among other things, some investors pulled out, including Francisco Partners selling their majority stake back to the founders.[50] In November 2021, the United States blacklisted NSO, practically banning it from doing business in the country.[51] While this act damaged NSO substantially, the firm seems to have remained active.[52] For instance, in 2023, the Citizen Lab researchers were able to identify spyware linked to the company in Apple devices once again.[53]

NSO's Pegasus is only one specific example of a product that is part of a much broader industry. Limiting Pegasus does not seriously limit the industry itself, nor the law enforcement practices that come with it. Though Pegasus is probably the best-known example, many other companies market similar products.

---

47. Julie Fuchs, *Is the EU protecting people from Pegasus spyware?*, ACCESS NOW (Mar. 17, 2023), www.accessnow.org/eu-pegasus-spyware/.

48. John Scott-Railton et al, *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, CITIZEN LAB (Feb. 11, 2017), www.citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/#:~:text=The%20targets%20of%20the%20Bitter,of%20sugary%20drinks%20in%20Mexico; John Scott-Railton et al., *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, CITIZEN LAB (June 19, 2017), www.citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ [hereinafter *Reckless Exploit*].

49. Ronen Bergman, *Exclusive: How Mexican drug baron El Chapo was brought down by technology made in Israel*, YNET (Oct. 1, 2019), www.ynetnews.com/articles/0,7340,L-5444330,00.html.

50. Amitai Ziv, *Israeli Cyberattack Firm NSO Bought Back by Founders at $1b Company Value*, HAARETZ (Feb. 14, 2019), www.haaretz.com/israel-news/business/2019-02-14/ty-article/.premium/israeli-cyberattack-firm-nso-bought-back-by-founders-at-1b-company-value/0000017f-e16f-d75c-a7ff-fdefa46b0000.

51. David E. Sanger, et al., *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. TIMES (Nov. 3, 2021), www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

52. *See* Jason Blessing, *A notorious Israeli spyware firm wants to use the Gaza war to make a comeback*, THE HILL (Jan. 27, 2024), www.thehill.com/opinion/cybersecurity/4433419-a-notorious-israeli-spyware-firm-wants-to-use-the-gaza-war-to-make-a-comeback.

53. Christopher Bing & Zeba Siddiqui, *New flaw in Apple devices led to spyware infection, researchers say*, REUTERS (Sep. 8, 2023), www.reuters.com/technology/new-flaw-apple-devices-led-spyware-infection-researchers-say-2023-09-07/.

Before Pegasus, the Italian firm Hacking Team was prominent in the cybersurveillance market (their databases have been leaked as well).[54] Quadream, another Israeli surveillance technology company, offered a similar program.[55] Candiru is another Israeli enterprise that was recently blacklisted by the United States because of its cybersurveillance products that allegedly threatened the national security of the United States.[56] Reporters have named several Israeli and U.S. companies that are trying to take over this market. Among these are Cytrox, Intelexa, Ocean's Edge, Leidos, Eqlipse Technologies, and more.[57] U.S. firms such as Boldend and Raytheon are in the business.[58] Perhaps most importantly from a U.S. perspective, Paragon, Israeli-made and U.S.-funded, is now seemingly prominent in this industry, as it has been reportedly acquired by a U.S. investment group for a few hundred million dollars.[59] However, Israeli reports claim the deal has not yet been approved by the Israeli regulators as required.[60] Based on public reports, Paragon's business model is aimed at selling its product to U.S. law enforcement agencies, and its focus is on complying with U.S. law and regulations.[61] Further, it has been reported that Paragon's

54. Lorenzo Franceschi-Bicchierai, *Hacking Team Founder: 'Hacking Team is Dead,'* VICE (May 26, 2020), www.vice.com/en/article/n7wbnd/hacking-team-is-dead.

55. Bill Marczak et al, *Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers*, CITIZEN LAB (Apr. 11, 2023), www.citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

56. Sanger et al., *supra* note 51.

57. Omer Kabir, הסייבר הישר אלי מצטמק: מ-18 ל-6 יצרניות רוגלה בתוך שנה [*Israeli Cyber Industry is Shrinking - from 18 to 6 Companies in a Year*], CALCALIST (Apr. 19, 2023), www.calcalist.co.il/calcalistech/article/rjdbgg3fn (Isr.).

58. Shannon Burton, *Pegasus and the Failure of Cybersurveillance Regulation*, 26 SAIS EUR. J. GLOB. AFF. 33, 34 (2023).

59. Thomas Brewster, *Meet Paragon: An American-Funded, Super-Secretive Israeli Surveillance Startup That 'Hacks WhatsApp And Signal,'* FORBES (July 30, 2021), www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/; A.J. Vicens, *Israeli spyware firm Paragon acquired by US investment group, report says*, REUTERS (Dec. 16, 2024) www.reuters.com/markets/deals/israeli-spyware-firm-paragon-acquired-by-us-investment-group-report-says-2024-12-16/.

60. Sophie Shulman, *Paragon's $900M sale in limbo as Defense Ministry steps in*, CALCALIST (Dec. 19, 2024), www.calcalistech.com/ctechnews/article/ryp3zcbhyl.

61. Mehul Srivastava & Kaye Wiggins, *Cyberweapon manufacturers plot to stay on the right side of US*, FIN. TIMES (May 31, 2023), www.ft.com/content/11cb394d-a13e-4826-b580-823b9367fedb; Mark Mazzetti et al., *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Jan. 28, 2023), www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

program, Graphite, has already been used by U.S. authorities.[62] And these are only the enterprises we know of.

By design, we do not fully understand how frequently or extensively U.S. law enforcement agencies are using these programs to gather evidence, nor how often courts encounter such evidence. While it had been reported that the FBI purchased Pegasus, and that other firms market their cybersurveillance products with U.S. law enforcement in mind,[63] the courts, by their nature, are reactive. Historically, legal doctrines concerning new technologies have been developed only after such technologies have been introduced and scrutinized in judicial proceedings. This Article advocates for equipping courts with the necessary legal frameworks to address these technologies when the inevitable legal challenges arise, while avoiding the mistakes other democratic nations have made when employing these technologies in criminal law enforcement. It explores the legal implications of these tools, assesses their global usage, predicts their potential application in the United States, and offers recommendations for how the U.S. legal system should adapt to this new era of cybersurveillance. But first, it is crucial to clarify what we currently know about these programs: how they operate and what they are capable of.

B. *How Does Pegasus Work?*

According to reports on Pegasus, the program had remarkably advanced capabilities.[64] Once a phone was infected with Pegasus, the program gained practically full access to that device.[65] But Pegasus is only one example of a product made by one company, which is part of a much larger industry.[66] This industry tends to be secretive by design and little is known about some of the products and the companies that comprise it. However, thanks first and foremost to analyses made by

62. Mark Mazzetti & Ronen Bergman, *Lawmakers Signal Inquiries Into U.S. Government's Use of Foreign Spyware*, N.Y. TIMES (Dec. 28, 2022), www.nytimes.com/2022/12/28/us/politics/spyware-israel-dea-fbi.html; Stephanie Kirchgaessner, *Ice obtains access to Israeli-made spyware that can hack phones and encrypted apps*, THE GUARDIAN (Sep. 2, 2025), www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware.

63. Bergman & Mazzetti, *Battle for the World's Most Powerful Cyberweapon, supra* note 38.

64. AMNESTY INTERNATIONAL, FORENSIC METHODOLOGY REPORT: HOW TO CATCH NSO GROUP'S PEGASUS 6 (2021), www.amnesty.org/en/documents/doc10/4487/2021/en/ [hereinafter HOW TO CATCH PEGASUS].

65. RICHARD & RIGAUD, *supra* note 11, at 6.

66. Press Release from David Agranovich & Mike Dvilyanski, *Taking Action Against the Surveillance-For-Hire Industry*, META (Dec. 16, 2021), www.about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/.

experts at Amnesty International and the Citizen Lab, who obtained phones infected with the spyware, there is publicly available information on Pegasus's forensics.[67]

Pegasus used vulnerabilities in other programs to gain access to users' phones. Initially, Pegasus was based on social engineering (rather than zero-click mechanisms).[68] Some versions of the program had to convince the target to click on a link for Pegasus to take over their device. As a result, the program would send a message to the target that was tailored to be a personalized bait.[69] For instance, when targeting members of crime organizations, the infection strategy was sometimes based on sending messages with reference to pornographic content.[70] In other cases, the message had to be more sophisticated. For example, Mexican journalist Jorge Carrasco received a message asking him to enter a webpage that looked like an article from Animal Politico, an investigative journalism website.[71]

More advanced versions were not dependent upon the operators' ability to conduct social engineering. NSO's ability to find zero-click vulnerabilities in common operating systems and applications, the holy grail of the cybersurveillance industry, allowed operators to break into phones without any need to convince the target to click on anything.[72] Amnesty International's forensic report noted that while malicious SMS messages were NSO's primary strategy between 2016 and 2018, they became rarer from 2019 onward.[73] That year, a zero-click vulnerability in Apple's iMessage application was widely used.[74] It was allegedly renewed in 2021.[75] NSO was able to spot and exploit similar vulnerabilities in other products. Forensic reports found that NSO could take over devices by simply calling them on WhatsApp, even if the target never answered.[76] Both Apple and WhatsApp later sued

67. *See* HOW TO CATCH PEGASUS, *supra* note 64*; see also Reckless Exploit*, *supra* note 48.

68. *See, e.g.*, Lee, *supra* note 15 (describing a social engineering incident).

69. RICHARD & RIGAUD, *supra* note 11, at 79-80.

70. *Id.* at 81.

71. *Id.* at 87.

72. *See BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild*, THE CITIZEN LAB (Sept. 7, 2023), www.citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.

73. HOW TO CATCH PEGASUS, *supra* note 64, at 16-17.

74. *Id.*

75. *Id.* at 21-22.

76. *WhatsApp attacked by advanced spyware*, DEUTSCHE WELLE (May 14, 2019), www.dw.com/en/whatsapp-attacked-by-advanced-spyware-via-missed-calls/a-48726819; Joe Tidy, *'I was a victim of the WhatsApp hack'*, BBC (Oct. 31, 2019), www.bbc.com/news/technology-50249859.

NSO.[77] Apple eventually dropped the lawsuit, but in 2025, a U.S. district court awarded WhatsApp with over $167 million in (mostly punitive) damages.[78]

Pegasus targets various operating systems, including Apple's iOS and Google's Android.[79] These companies issue updates to their systems regularly, shutting down vulnerabilities. Pegasus was accordingly in need of constant changing, adapting to updated operating systems, and finding their new vulnerabilities. In April 2023, the Citizen Lab reported that it had found another zero-click exploit used by Pegasus in the iOS operating system.[80]

Public knowledge of what exactly the system looks like from the operator's side is limited. Some reports point out that operators needed to install hardware on their end, for instance, by the fact that the FBI had to "unpack dozens of computer servers" to be able to deploy Pegasus from their New Jersey office.[81] In 2018, a VICE reporter spoke to a source who saw a live demo of NSO's Pegasus.[82] This source described giving NSO his phone number as part of the demonstration of the program. Within minutes, the contents of his phone appeared on a large screen. The interface included icons of various applications, including SMS messages and emails.[83] He further described that NSO representatives were able to access "any information that was on my [iPhone]" and that they could access his microphone and camera as well.[84]

---

77. Stephanie Kirchgaessner, *WhatsApp: Israeli firm 'deeply involved' in hacking our users*, THE GUARDIAN (Apr. 29, 2020), www.theguardian.com/world/2020/apr/29/whatsapp-israeli-firm-deeply-involved-in-hacking-our-users; Press Release, Apple, Apple sues NSO Group to curb the abuse of state-sponsored spyware (Nov. 23, 2021), www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/.

78. Jury Verdict, *WhatsApp Inc. v. NSO Group Technologies Ltd.*, No. 4:19-cv-07123 (N.D. Cal. May. 6, 2025); Joseph Menn, *Apple seeks to drop its lawsuit against Israeli spyware pioneer NSO*, THE WASHINGTON POST (Sep. 13, 2024), www.washingtonpost.com/technology/2024/09/13/apple-lawsuit-nso-pegasus-spyware/.

79. *See* RICHARD & RIGAUD, *supra* note 11, at 79.

80. Bill Marczak et al., *Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*, THE CITIZEN LAB (Apr. 18, 2023), www.citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/.

81. Bergman & Mazzetti, *Battle for the World's Most Powerful Cyberweapon*, *supra* note 38. *See also* Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*, N.Y. TIMES (Nov. 15, 2022), www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html.

82. Lorenzo Franceschi-Bicchierai & Joseph Cox, *They Got 'Everything': Inside a Demo of NSO Group's Powerful iPhone Malware*, VICE (Sept. 20, 2018), www.vice.com/en/article/inside-nso-group-spyware-demo/.

83. *Id.*

84. *Id.*

A similar description appears in a book by the journalists who led the Pegasus Project. A person identified as "Jose" was among Pegasus's operators in Mexico.[85] He is described as one of the very few people trained to operate the system.[86] He, too, said that NSO's operations demanded a considerable amount of hardware to be installed, including an uninterrupted power system, modems, servers, and routers.[87] After a device has been infected, Pegasus generated a screen of modules mapping the infected device, including:

> A series of small boxes on the right half of the screen, each representing a separate application at work on the phone. There might be a box for WhatsApp, or for Signal, or for any other messaging app (encrypted or not) that contained every message archived on the phone and every message in or out since infection. Messages deleted after infection became faint on Jose's screen, almost ghostly, but still readable. There was a box for email; one for calls, call history, and voice messages; one for real-time geolocation and geolocation history; one for the device's microphone; and one for the device's camera. Jose could then choose any app he wanted to check or monitor, and it would expand into an easily readable box on the left of the screen.[88]

Based on the existing body of literature and coverage, I suggest that Pegasus's technical abilities could be classified into three broad categories: access to live data as it is being created after the infection; access to data stored on the device that was created before the infection, including the ability to erase contents; and the capability to create new content without the user's knowledge or consent, using the infected device's microphone and camera.

First, operators could surveil and follow new data as it was being created after the infection.[89] Unlike the typical computer search, in which a device is seized and its contents are searched but no new data is created and stored on it, Pegasus allowed its operators to watch and search new materials as they were being created, sent, and received by the infected device, without the user's consent or awareness. This mechanism

85. RICHARD & RIGAUD, *supra* note 11, at 77.

86. *Id.*

87. *Id.* at 80.

88. *Id.* at 81.

89. *Id.*; Rich Cannings et al., *An investigation of Chrysaor Malware on Android*, GOOGLE ANDROID DEVELOPER BLOG (Apr. 3, 2017), www.android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html, *see also* Pegg & Cutler, *supra* note 2.

could be perceived as similar to wiretapping, only with access to a much wider pool of information. Among the data are not only messages coming in and out but also messages that came in or were sent out and then deleted if the phone was infected before the deletion.[90] It allowed the operator to record calls as well.[91] The program also showed the operator the live geolocation of the infected device on a map, making the target trackable after the infection.[92]

Second, Pegasus allowed operators to access stored content on infected devices. It could access apps such as WhatsApp, iMessage, and email.[93] Further, Pegasus allowed the operators to collect contents such as passwords and geolocation.[94] It also gained access to the contact list saved on the phone, call history, and voice messages.[95] It allowed the operator to view and save content stored on the infected device remotely.

Some reports have claimed that Pegasus was able not only to view but also to delete files from infected devices. A Rwandan exile living in Leeds who was, according to the BBC, targeted by Pegasus, reported that he understood "something was wrong" only after he discovered that files disappeared from his device.[96] This ability made Pegasus much harder to detect because the operator was able to remove files that contained traces of the spyware's existence on the device (NSO Group claimed it "leaves no traces", though later forensics reports differed).[97] A report by the Citizen Lab and Amnesty International adds that NSO Group implemented a "clean-up step, which deletes browser cache files and other artifacts that could reveal the attack vendor."[98]

Third, the program allowed operators to create new content using the infected devices. For instance, operators could access the camera of a phone remotely and record everything that happens in its

90. RICHARD & RIGAUD, *supra* note 11, at 81.

91. Pegg & Cutler, *supra* note 2.

92. *See id.*

93. *Id.*

94. Charles Whitmore, *Pegasus spyware: what do you need to know?*, NORDVPN (Mar. 2, 2024), www.nordvpn.com/he/blog/pegasus-spyware. RICHARD & RIGAUD, *supra* note 11, at 81.

95. RICHARD & RIGAUD, *supra* note 11, at 81.

96. Tidy, *supra* note 76.

97. *See, e.g.*, *ETtech Explainer: What is Pegasus spyware and how it works*, ECON. TIMES (July 21, 2021), www.economictimes.indiatimes.com/tech/trendspotting/what-is-pegasus-spyware-and-how-it-works/articleshow/84607533.cms; HOW TO CATCH PEGASUS, *supra* note 64, at 25.

98. Donncha O'Cearbhaill & Bill Marczak, Exploit Archaeology: A Forensic History of In-the-Wild NSO Group Exploits, 12 (2022) (unpublished paper presented at the 2022 International Virus Bulletin Conference), web.archive.org/web/20250504124237/www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Exploit-archaeology-a-forensic-history-of-in-the-wild-NSO-Group-exploits.pdf.

surroundings, even if the user never launched the camera.[99] As Jose described it to Laurent Richard and Sandrine Rigaud, "[i]f I wanted, for example, the front-facing camera, I would tap on the front-facing camera, and it would magnify the front-facing camera image for me."[100] According to Richard and Rigaud, "he could, even from his seat, turn on the remote microphone and listen to any real-time conversation within earshot of the phone."[101] VICE's source, who was exposed to a demo of Pegasus, witnessed similar features.[102] This category of capabilities raises uniquely complex legal questions. I suggest that, in this situation, it is not the *phone* that is being searched by the operator, but rather its physical surroundings.

Each of these three categories of capabilities raises unique legal questions. This Article discusses these implications in detail in the following parts, making the point that it is doctrinally incorrect to treat Pegasus and similar programs as one singular tool. Instead, they should be perceived as an entire toolbox with diverse features.

C. *The "Going Dark" Argument*

Perhaps the most common argument put forth by NSO and similar firms in support of employing this new suite of cybersurveillance tools is not that the government must expand its surveillance capabilities, but rather that it must preserve its existing abilities. These firms contend that such tools are essential to ensure law enforcement does not "go dark," or lose the capacity to monitor suspects as technology evolves. For instance, the way NSO's founder, Hulio, recounted the story, he first realized that he could sell their product, originally marketed as a tool to help support technicians serve customers, to law enforcement and national security agencies after a European intelligence service approached them. In a 2019 interview, well before the Pegasus Project was published, Hulio described the conversation he had with that officer:

99. Stephen Shankland, *Pegasus Spyware and Citizen Surveillance: Here's What You Should Know*, CNET (July 19, 2022), www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/; *Emergency Update for All Apple Users: Everything You Need to Know About Pegasus Spyware*, AMNESTY INT'L (Sept. 23, 2021), www.amnesty.org.au/everything-you-need-to-know-about-pegasus-spyware/.

100. RICHARD & RIGAUD, *supra* note 11, at 81.

101. *Id.*

102. Franceschi-Bicchierai & Cox, *supra* note 82.

> "A European intelligence service heard what we were doing and approached us," Hulio says. "'We saw that your technology works . . . why aren't you using this to collect intelligence?'
>
> "Truthfully, we didn't really understand what they wanted. We said [to the officer]: 'What's your problem in collecting intelligence? You sit inside the cell phone carrier.' They said we didn't really understand, that the situation was grave. 'We are going dark. We are going blind,' were the exact words they used. 'Help us.'"[103]

Hulio was, of course, marketing a product in this interview, and it is practically impossible to verify whether the conversation he described actually occurred. However, the story indicates a real challenge facing law enforcement agencies. That problem is the growing use of encryption and the declining power of cellular carriers. Wiretapping, pen registers, or Cell Site Location Information (CSLI) are no longer as effective.[104] Messages and calls sent through WhatsApp, Signal, Telegram, and similar products are typically no longer accessible to cellular carriers, primarily due to the encryption they offer.[105]

To put it differently, these messages are typically not accessible to anyone except the sender and the recipient. To obtain their contents, law enforcement agencies cannot ask the cellular carrier or the software provider to disclose the contents. Law enforcement agencies then may indeed "go dark" or "turn blind." If they do not regain the ability to access that information, they may effectively lose their ability to obtain communication evidence. The way around it is primarily through offensive, cybersurveillance operations such as Pegasus. If those technologies will not be used whatsoever, criminals will just use encrypted communications, which are readily accessible and often free, to largely avoid surveillance by law enforcement.

---

103. Ronen Bergman, *Weaving a cyber web*, YNET (Nov. 1, 2019), www.ynetnews.com/articles/0,7340,L-5444998,00.html.

104. *See* John M. Traylor, *Shedding Light on the "Going Dark" Problem and the Encryption Debate*, 50 U. MICH. J. L. REFORM 489, 491-494 (2016). *See also* James B. Comey, Dir., Fed. Bureau of Investigation, Remarks at the Brookings Institution: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, (Oct. 16, 2014), (transcript available at www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course) (discussing what happens when a potential suspect switches from cellular coverage to Wi-Fi, or from cellular voice service to an app).

105. *See* RICHARD & RIGAUD, *supra* note 11, at 53; *see, e.g.* WhatsApp Help Center, *Information for Law Enforcement Authorities*, WHATSAPP (Last retrieved: June 24, 2024), faq.whatsapp.com/444002211197967.

Indeed, Pegasus and equivalent programs offer much more than wiretapping live communications. As reviewed, they can also access stored content and generate new information. To some extent, these features have existing equivalents: the police can storm into a house and access diaries with "stored content," or install hidden cameras in a house. But these practices are limited, closely regulated, and treated very seriously by the courts. They are not illegitimate *per se*, but they are often illegal unless the government can clearly justify them. Pegasus, I argue, is not fundamentally different from these practices and therefore is not *necessarily* illegitimate. The way it is used matters.

These practices can only be justified if Pegasus is treated as it is: an extremely powerful law enforcement tool,[106] that allows the government to conduct highly sensitive and invasive searches. These tools could be legitimately used in law enforcement, and they can be illegitimately abused, much like many other law enforcement practices. The legitimacy comes not from the tool, but from the way it is being used. The legitimacy is not just about the spyware, but rather about the circumstances in which it is used, like the nature of the investigated crime, the nature of the agency, the efficacy of the regulation imposed on the tool, and the nature of the tool and its specific features.

III. A Comparative View

Democracies other than the United States, including Israel and various European countries, have previously confronted the legal challenges posed by the use of cyber operational tools. Two specific documents are particularly relevant for U.S. legal stakeholders: the Merari Report, issued by the Israeli Ministry of Justice,[107] and the PEGA Report, published by the European Parliament.[108] Based on these reports, this section introduces the key themes through which Israel and the EU addressed the legal dilemmas arising from tools such as Pegasus, highlighting potential lessons for U.S. policymakers.

106. Burton, *supra* note 58, at 34-35 (referring to Pegasus as "cyberweapon").

107. Merari et al., *supra* note 40.

108. Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the use of Pegasus and Equivalent Surveillance Spyware*, Eur. Parl. Rep. A9-0189/2023 (2023), www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html [hereinafter PEGA report].

A. *Israel's Merari Report*

Israel faced legal and regulatory challenges posed by Pegasus and the cybersurveillance spyware industry because, among other reasons, many of these programs are developed in Israel by Israelis. This section briefly covers Israel's relevant regulatory framework, the revelations on how Pegasus has been used in Israel and the findings of a report issued by a committee appointed by the Attorney General to investigate the reports on the spyware's potential abuse.

1. NSO and Israel's Defense Export Control

The fact that Pegasus was developed in Israel by NSO, a company incorporated in Israel, posed challenges that the Israeli administrative and legal system had to address long before the full extent of Pegasus's capabilities became public knowledge. NSO's entire business model relied on exporting the program abroad and selling it to foreign governments outside of Israel. Under Israel's Defense Export Control Law, strict regulatory standards are imposed on companies seeking to export weaponry, including "Defensive Knowledge" and "Defensive Services."[109] Companies intending to export products, knowledge, or training deemed of a "defensive nature" by the Israeli Ministry of Defense must obtain a license from the Defense Export Controls Agency (DECA).[110] Furthermore, each transaction and client must be vetted by DECA, based on considerations prioritizing Israel's national security and other interests defined by law.[111]

NSO obtained licenses from DECA, and its export of Pegasus seemingly complied with Israeli law.[112] However, in 2021, following the global Pegasus scandal, the Ministry of Defense imposed new restrictions and regulations on cyber warfare tools.[113] Despite these measures, some Israeli legal scholars argued that the regulations were still insufficient. Critics suggested that DECA should consider not only national

109. Defense Export Control Law, 5776-2007, art. 1 (2007) (Isr.).

110. *Id.* art. 3.

111. *Id.* arts. 1, 4.

112. *See* Judah Ari Gross, *Amid fallout from NSO scandal, Israel imposes new restrictions on cyber Exports*, TIMES OF ISR. (Dec. 6, 2021), www.timesofisrael.com/amid-fallout-from-nso-scandal-israel-imposes-new-restrictions-on-cyber-exports/.

113. Yoav Zeitoun, משרד הביטחון מהדק את הפיקוח על ייצוא מערכות: על רקע פרשת אן.אס.או [*Following the NSO Affair: The Ministry of Defense Tightens Regulations on Cyber Exportation*], YNET (Dec. 6, 2021), www.ynet.co.il/news/article/rjcafaikf (Isr.).

security and diplomatic relations but also the risks of human rights violations and explicitly defined international standards.[114]

Reports indicate that Israel not only permitted NSO to sell its products to authoritarian regimes, such as the UAE, but actively encouraged these sales to achieve diplomatic and political goals.[115] For instance, Israel reportedly leveraged NSO's products to secure diplomatic gains and promote unrelated political interests in regions like Latin America.[116]

Within Israel, NSO also marketed Pegasus to domestic agencies,[117] which did not require an export license to operate within Israel's governmental ecosystem. Because Pegasus' developers were largely veterans of the Israel Defense Forces (IDF), whose knowledge in the field may derive from tools developed during their service, it was probable Israel employed similar programs in military and national security contexts. Recent reports suggest, for example, that the Israeli military has used Pegasus to try to locate Israeli hostages held in Gaza.[118]

However, the use of these tools by Israeli agencies was not limited to national security. Their deployment in ordinary, criminal law enforcement operations sparked significant political controversy.[119] The revelation that Israeli authorities utilized tools like Pegasus for domestic law enforcement purposes caused widespread public and political turmoil, challenging the long-standing assumption that such tools were mostly reserved for defense or national security purposes.[120]

---

114. *See* Hilla Goldschmid, סייבר התקפי – בין יצוא בטחוני לייבוא אכיפתי [*Offensive Cyber Operations – Between Security Exports and Enforcement through Importation*], TEL AVIV L. REV. ONLINE (Jan. 20, 2022), www.taulawreview.sites.tau.ac.il/post/goldschmid (Isr.).

115. *See* Aluf Benn, *Netanyahu Used NSO's Pegasus for Diplomacy. Now He Blames It for His Downfall*, HAARETZ (Feb. 5, 2022), www.haaretz.com/israel-news/2022-02-05/ty-article/.premium/netanyahu-used-nsos-pegasus-for-diplomacy-now-he-blames-it-for-his-downfall/0000017f-e941-dc91-a17f-fdcd55c80000; Mazzetti et al., *supra* note 61.

116. Burton, *supra* note 58, at 33-34.

117. *See* Shira Rubin, *Israeli police accused of using Pegasus spyware on domestic opponents of Netanyahu*, WASH. POST (Jan. 18, 2022), www.washingtonpost.com/world/2022/01/18/israel-pegasus-activists-spyware.

118. Gwen Ackerman & Marissa Newman, *Israel Taps Blacklisted Pegasus Maker to Track Hostages in Gaza*, BLOOMBERG (Oct. 26, 2023), www.bloomberg.com/news/articles/2023-10-26/israel-taps-blacklisted-pegasus-maker-nso-to-track-gaza-hostages-and-hamas.

119. *See* Anshel Pferffer, *Israelis Didn't Care About NSO and Pegasus - Until This Scandal*, HAARETZ (Feb. 6, 2022), www.haaretz.com/israel-news/2022-02-06/ty-article/.premium/israelis-didnt-care-about-nso-and-pegasus-until-this-scandal/0000017f-e857-dea7-adff-f9ff5c1d0000.

120. *See id.*; Daniel Estrin, *Israeli police used spyware to hack its own citizens, an Israeli newspaper reports*, NPR (Jan. 18, 2022), www.npr.org/2022/01/18/1073828708/israel-spyware-citizens-nso-group (discussing the alleged limited authority of the police, in contrary to the Shin Bet, to use Pegasus).

2. The Calcalist Reportage

On January 18, 2022, the Israeli financial newspaper Calcalist reported that the Israeli police had used Pegasus extensively.[121] The program was employed to obtain evidence and surveil suspects.[122] The list of individuals allegedly surveilled using the spyware initially shocked many. Calcalist reported that those purportedly targeted included political activists opposing Prime Minister Benjamin Netanyahu, civil servants accused of fraud, an elected mayor allegedly bribed by a contractor, individuals suspected of murder, and anti-LGBTQ activists.[123] The report further alleged that the police used Pegasus without obtaining judicial warrants.[124]

In February 2022, Calcalist published a follow-up article titled "Pegasus Reached Everyone."[125] This story claimed that the Israeli police had used Pegasus in a wide range of highly sensitive cases. Among the alleged targets were heads and directors of government agencies, prominent businessmen, and—perhaps most politically sensitive—aides to Prime Minister Netanyahu, including his son, Avner.[126] The article suggested that Pegasus was employed so extensively that it targeted both dissidents and senior members of the government, journalists, and corrupt businesspeople.[127]

At first, the police categorically denied the story.[128] A spokesperson for the Israeli police described the allegations as "baseless" in their initial response to the original report.[129] Later that same month, former Chief of Police Roni Alsheikh, who was in office at the time of the alleged incidents, stated that the police did not have access to Pegasus or any cybersurveillance tool with the ability to obtain content retroactively, meaning content created before the spyware infected a device. "To clear any doubts," Alsheikh said, "the Israeli police do not have Pegasus."[130]

---

121. Ganon, *NSO in the service of the Israeli police, supra* note 39.

122. *Id.*

123. *Id.*

124. *Id.*

125. Tomer Ganon, ממנכ"לים של משרדי ממשלה ועד עיתונאים ואנשי עסקים: ההדבקה ההמונית בפגסוס הגיעה לכולם [*Directors of Government Offices, Journalists, and Businesspeople: Pegasus Reached Everyone*], CALCALIST (Feb. 7, 2022), www.calcalist.co.il/local_news/article/s1ziccp0f (Isr.).

126. *Id.*

127. *Id.*

128. Yaniv Kobuvitz, אלשיך: למשטרה אין פגסוס,ה סיפור הזה הוא ספין [*Elsheich: The Police Does Not Have Pegasus, this Story is a Spin*], HAARETZ (Feb. 13, 2022), www.haaretz.co.il/news/law/2022-02-13/ty-article/0000017f-e92f-dea7-adff-f9ff642f0000 (Isr.).

129. Ganon, *NSO in the service of the Israeli police, supra* note 39.

130. Kobuvitz, *supra* note 128.

3. The Merari Report

The political uproar generated by these revelations led the Attorney General to appoint a special investigative team, headed by Deputy Attorney General Amit Merari.[131] Quite swiftly, by mid-February, the Merari Committee released its initial findings. The committee confirmed that the police had indeed used a version of NSO's Pegasus, called "Sayfan."[132] However, it also concluded that many of the allegations in the Calcalist reports were unfounded.[133] For example, the investigation found no evidence that the police had infected the devices of the individuals explicitly named in the publications, or that it systematically employed Pegasus infections without warrants.[134]

In light of these findings, Calcalist issued a statement emphasizing that "despite their initial denial, there is no doubt anymore that the police used spyware to infect the phones of Israeli citizens."[135] However, the statement also acknowledged that "there might be a possibility that the list [of people allegedly surveilled] was not accurate."[136]

The Merari Committee continued its work, and its complete and detailed findings were published in August 2022.[137] The report not only fueled ongoing public and political debate but also shed new light on the extent to which Israeli authorities relied on cybersurveillance in criminal contexts.

a. Main Factual Findings

The Merari Report was authored by the three members of the investigative committee: Deputy Attorney General for Criminal Matters Amit Merari (chair), Eyal Dagan (former head of the investigations department of the Israeli internal security service, the Shin Bet), and Zafrir

131. Chen Maanit, *Israel to Investigate Police Use of NGO's Pegasus Spyware*, HAARETZ (July 20, 2023), www.haaretz.com/israel-news/2023-07-20/ty-article/.premium/israel-to-investigate-police-use-of-ngos-pegasus-spyware/00000189-74c0-d09f-a3a9-f7e921120000.

132. MERARI ET AL., *supra* note 40, at 2; Yuval Erel et al., את ממצאי התחקיר : אין עדויות שהמשטרה התקינה פגסוס לאנשים שפורסמו ועדת מררי דוחה [*The Marari Committee rejects the findings: There is no evidence that the police installed Pegasus on the individuals mentioned*], N12 (Feb. 21, 2022), www.mako.co.il/news-israel/2022_q1/Article-2381273e41d1f71027.htm (Isr.).

133. Erel et al., *supra* note 132.

134. *Id.*

135. Chen Maanit, *Calcalist: The Pegasus Story is Based on Testimony from the Cyber Department, We Might Have Been Wrong regarding the List*, HAARETZ (Mar. 14, 2022), www.haaretz.co.il/news/law/2022-03-14/ty-article/.premium/00000180-5b8b-dc4e-a5a9-7fff9d0b0000.

136. *Id.*

137. MERARI ET AL., *supra* note 40.

Katz (former head of the technologies department at the Shin Bet).[138] The report was published after a comprehensive review of data and consultations with relevant parties, including the police, NSO, different NGOs, and Calcalist. It also included a detailed examination of the relevant statutory framework of Israeli law.[139]

The Merari Committee found that, despite the claims made by the former Chief of Police, the Israeli police had access to a version of Pegasus, known as Sayfan.[140] This program was capable of obtaining content created prior to the issuance of a warrant and retroactively retrieving information in ways that were inconsistent with Israeli law.[141] However, the report also determined that contrary to the claims in the Calcalist revelations, all infections except for four were conducted pursuant to lawfully issued court warrants.[142] In the four particular cases where no warrants were issued, the infections ultimately failed and thus the spyware was unable to retrieve content.[143]

The committee also found that Sayfan's ability to retrieve information created before the infection, as well as its capability to access non-communication data, was not compliant with Israeli law.[144] The committee recommended ensuring that judges fully understand the implications of the warrants they issue, particularly when approving the use of Pegasus, as these motions were often presented as requests for "regular wiretapping."[145] It further advised revising Israel's outdated Wiretap Law, which currently regulates mostly traditional wiretaps, to explicitly address and govern newer technologies like Pegasus.[146] Additionally, it clarified that the police's access to such programs should be restricted to ensure compliance with Israeli legal standards.[147]

It is worth noting that Israeli media later claimed that, in at least one case, evidence obtained unlawfully by spyware was excluded in court.[148] While the police typically obtained warrants before conducting searches

138. *Id.*
139. *Id.* at 1-3.
140. *Id.* at 2.
141. *Id.* at 4-6.
142. *Id.* at 29.
143. *Id.*
144. *Id.* at 5-6.
145. *See id.* at 7.
146. *Id.* at *9.*
147. *Id.* at 6.
148. Yuval Erel et al., באופן חריג: המדינה נאלצה למשוך ראיות בתיק רצח כפול - כי הושגו בשימוש לא חוקי בתוכנות רוגלה [*Prosecution to retract evidence in a double murder case, because it was unlawfully obtained using malware*], N12 NEWS (June 5, 2023), www.mako.co.il/news-law/2023_q2/Article-f86f426376a8881026.htm (Isr.).

with Pegasus, if that report is accurate, at least one case required the prosecution to withdraw evidence obtained through the program or a similar program. According to a report by Israel's Channel 12, the prosecution had to retract evidence in a double murder case because the information had been obtained unlawfully through the use of spyware.[149] The report further stated that the State Attorney's Office reviewed twenty-seven additional cases where spyware had allegedly gathered information not covered by warrants.[150] However, it concluded that this evidence had never been introduced in legal proceedings and thus did not require retraction.[151] The Merari Report was published before these claims had been reported in the media and does not address this particular case.

The Merari Report does provide a series of recommendations addressing the police's cybersurveillance practices more broadly. To fully understand these recommendations, a brief introduction to the Israeli statutory framework is in order.

b. Israeli Statutory Framework

The primary statute that governs surveillance practices in Israel is the Wiretap Law of 1979.[152] The law generally prohibits unauthorized wiretapping and stipulates that the punishment for illegal wiretapping is up to five years in prison.[153]

Article 4 allows wiretapping in some rare situations, specifically in matters of national security.[154] Article 6 regulates the situations in which the police may be authorized to conduct wiretapping in connection with criminal investigations.[155] According to the law, the chief judge of a district court (generally equivalent to a court of appeals) may permit the police to wiretap a line in the investigation of a crime punishable by more than three years in prison.[156] Article 7 provides an exception that allows wiretapping without a warrant in cases where the Chief of Police deems it urgently necessary to prevent a serious crime or to identify the perpetrator of a serious crime.[157] However, such wiretapping may not exceed forty-eight hours.[158] The Chief of Police is also

149. *Id.*
150. *Id.*
151. *Id.*
152. Secret Monitoring Law, 5739–1979, SH 50 141 (Isr.).
153. *Id.* art. 2.
154. *Id.* art. 4.
155. *Id.* art. 6.
156. *Id.*
157. *Id.* art. 7.
158. *Id.*

required to notify the Attorney General of such a decision, and the Attorney General is authorized to annul the wiretap.[159]

The original definition of the term "wiretap" in Israeli law focused on conversations conducted "through talking or another form of communication."[160] In a 1995 amendment, the law explicitly added that a conversation could occur "between computers."[161] Israel's Computer Law defines a computer as a device "that operates using software to perform arithmetic or logical processing of data."[162] By this definition, a smartphone qualifies as a computer.

As the Merari Report noted, Israeli law draws a distinction between a wiretap and a search of computer materials.[163] Once data has been stored and the communication has ended, Israeli law treats that data as an "item."[164] Accordingly, the search of such data falls under a different statutory framework: the Criminal Procedure Ordinance (Arrests and Searches) of 1969.[165] Notably, a search under the Ordinance is typically conducted visibly, meaning the suspect is typically made aware that their data is being searched, or through the issuance of a subpoena directed at the person controlling the data or item.[166] In other words, Israeli police officers are authorized to obtain communications content without the user's knowledge mostly through live wiretapping, that is, while the communication is occurring. They are not authorized to obtain the data after the communication has concluded using techniques of a wiretapping nature, such as Pegasus infections. Such retrieval of stored data is permissible only as part of a visible search conducted under the framework of the Ordinance.

Another set of procedural rules allows the police to obtain metadata through cellphone carrier companies. The Criminal Procedure Law (Enforcement Authorities – Communication Data) of 2007 permits the police to request a warrant to obtain metadata, including CSLI, subscription information, and other technical details.[167] This statute also authorizes the police to access these data without a warrant in emergency situations.[168] However, it does not allow access to the contents of communications.

159. *Id.*
160. Id, art. 1.
161. *Id.*
162. Art. 1, Computers Law, 5755-1995 (Isr.).
163. *See* MERARI ET AL., *supra* note 40, at 21-23.
164. *Id.* at 21.
165. Criminal Procedure Ordinance (Arrests and Searches), 5729-1969, (Isr.).
166. *See id.* arts. 23, 26; MERARI ET AL., *supra* note 40, at 21-22.
167. Criminal Procedure Law, 5768-2007, arts. 1, 3 (Isr.).
168. *Id.* art. 4.

c. Recommendations

The Merari Report provides a set of practical recommendations across three main levels. First, it addresses the relationship between Israeli law enforcement and private firms that sell surveillance software, requiring redesigning the software to fit Israeli legal standards.[169] Second, it focuses on judicial and administrative oversight of the police's conduct in cybersurveillance.[170] Third, it makes recommendations on the legislative level, advocating for further amendments to ensure that Israeli criminal procedure rules align with the realities of emerging surveillance technologies.[171]

On the first and most immediate level, the report recommends that the police ensure they only access programs with capabilities that are in full compliance with Israeli law.[172] For example, Pegasus was able to obtain access to stored content created before the infection of the device and before the issuance of a warrant—a capability that does not comply with Israeli law. As noted earlier, Israeli law does not permit searches of stored content through secretive wiretapping.[173] Therefore, the police should not acquire programs with these capabilities and should instead negotiate to create a variant of Pegasus that fits within the jurisdictional legal framework.

The report specifically highlights two categories of content that Pegasus could access but Israeli law does not authorize. The first category is stored communications, meaning communications created and transmitted before the issuance of a warrant and the infection of the device.[174] Although the committee found no evidence that the police had used Pegasus to access such content, the program's ability to do so theoretically still violated legal standards.

The second category involves information that does not constitute communication at all and, as such, should not be obtained under wiretapping laws.[175] For example, upon infection, Pegasus automatically disclosed the list of applications installed on the device to the operator.[176] Additionally, the program was capable of accessing notes, calendar

169. MERARI ET AL., *supra* note 40, at 6.
170. *Id.* at 6-7.
171. *Id.* at 7-9.
172. *Id.* at 6.
173. *See id.* at 21-23.
174. *Id.* at 37-38.
175. *Id.* at 38-40.
176. *Id.* at 38.

entries, contact lists, and other forms of stored data, upon command.[177] While the feature automatically obtaining the application list was deemed essential for the spyware's functionality—and might under certain circumstances be accordingly lawful—the report finds that other categories of stored data should not be accessible through such programs at all.[178] The committee recommended that every capability not explicitly authorized by Israeli law should be blocked.[179] Furthermore, it suggested that even the automatically obtained list of applications, while technically crucial for the program's operation, should not be automatically accessible to human beings, including the officers.[180]

On the second level, addressing judicial and administrative oversight of the police's use of these programs, the report offers several recommendations. First, it emphasizes that the way these programs operate should be communicated more precisely to judges.[181] Currently, the forms used by the police when seeking warrants note that a program will be installed on a suspect's phone to facilitate wiretapping.[182] However, the committee found that these forms did not adequately explain to judges how the program works or what it allows the police to do.[183] The committee recommended that the police provide judges with more detailed explanations of the program's functionalities before obtaining warrants under the Wiretap Law.[184] The report also recommends workshops or conferences to educate judges about modern surveillance technologies.[185] These educational efforts would ensure that judges better understand the capabilities of the programs they are authorizing.

Additionally, the report proposes amending internal police protocols to ensure that officers responsible for cybersurveillance strictly adhere to the relevant procedures.[186] Similarly, the report recommends strengthening the regulation exercised by the Israeli Ministry of Justice over police practices in this area.[187] It notes that the police must obtain

177. *Id.* at 38-39.

178. According to the report, since obtaining the application list was required for the functionality of the program, it could have been lawful in certain situations, for instance, if the list was retained at the hands of the police technical experts, and not disclosed to the investigative crew. *Id.* at 38-41.

179. *Id.* at 6, 37-39.

180. *Id.* at 42.

181. *Id.* at 46-48.

182. *Id.* at 46-47.

183. *Id.*

184. *Id.*

185. *Id.* at 47.

186. *Id.* at 52.

187. *Id.* at 60.

authorization from the Attorney General before purchasing and deploying surveillance programs.[188] The committee further suggested that police legal advisors and Ministry of Justice officials should be closely involved in reviewing and implementing such systems to ensure compliance with Israeli legal standards.[189]

On the third level, addressing legislative reforms, the committee called upon lawmakers to amend existing laws to align them with modern technological developments. Although the committee refrained from endorsing specific legislative amendments, it acknowledged the various proposals put forth by NGOs and stressed the urgent need to review the law.[190] The report highlights that the Wiretap Law, originally enacted in the 1970s and amended in the 1990s, has not kept pace with technological advancements.[191] As a result, the committee found it necessary to revise and update the law to address contemporary challenges in cybersurveillance.[192]

4. The Drori Committee and Pending Legislation

The Merari Report sparked significant debate within the Israeli political system. One of the first points of contention was the extent to which the Calcalist reports were accurate and fair. The newspaper itself asserted that the Merari Report revealed "severe violations of privacy and suspects' rights."[193] It further described the findings as "only the beginning," insisting that the report should lead to comprehensive legal reforms and potentially criminal investigations.[194] On the other hand, other media outlets focused on the report's conclusion that many of the claims made in Calcalist's earlier publications were found to be inaccurate.[195]

The controversy quickly escalated into a political battle between opposing camps, particularly concerning reports that one of the

---

188. *Id.*

189. *Id.* at 60-62, 68.

190. *Id.* at 69-70.

191. *Id.*

192. *Id.*

193. Tomer Ganon, דו"ח מררי: הממצאים החמורים הם רק ההתחלה [*The Merari Report: The Serious Findings are Merely the Beginning*], CALCALIST (Aug. 2, 2022), www.calcalist.co.il/local_news/article/rjcl35baq (Isr.).

194. *Id.*

195. *See, e.g.*, Gur Megido, צריך לקרוא לזה "פרשת כלכליסט". הממצא העיקרי: כמה קל לשחק לכולנו בתודעה [*This Should Be Called Calcalist-Gate, The Main Finding is How Easy it is to Play with Our Minds*], THE MARKER (Aug. 1, 2022), www.themarker.com/opinion/2022-08-01/ty-article/.highlight/00000182-5a29-d9b3-a1a2-5bf944a60000 (Isr.).

individuals allegedly infected by Sayfan was Shlomo Filber, a former senior official closely associated with Prime Minister Benjamin Netanyahu.[196] Filber later became a state witness against Netanyahu, though he is still perceived to be politically supportive of him, and the prosecution eventually annulled his state witness agreement after he contradicted his initial testimonies against Netanyahu in court.[197] This revelation became a central issue in Netanyahu's trial, with Netanyahu's legal team using the infection of Filber's phone with the spyware as a prominent line of defense.[198] Netanyahu's supporters subsequently called for a wider and more thorough investigation into the use of Pegasus by the police, arguing that the Merari Report had not gone far enough.[199]

Eventually, Netanyahu's cabinet decided to establish an additional committee of inquiry, chaired by retired conservative judge Moshe Drori, to investigate the deployment of cybersurveillance in criminal investigations in Israel.[200] The formation of the Drori Committee was met with sharp criticism from opposition leaders, as well as the Attorney General and the Shin Bet.[201] Petitions were filed with the Supreme Court alleging that the committee was unlawfully examining aspects of Netanyahu's ongoing criminal trial.[202] The Supreme Court ruled that the Drori Committee must refrain from interfering in pending criminal proceedings.[203] Nevertheless, the Attorney General later claimed that the committee continued to investigate

---

196. Tova Zimoki & Gilad Morag, המשטרה השתמשה בפגסוס בחקירות פילבר, הפרקליטות נערכת לעדותו [*The Police Used Pegasus in the Filber Investigation, the Prosecution is Preparing to His Testimony*], YNET (Mar. 2, 2022), www.ynet.co.il/news/article/bjckn00yrf (Isr.).

197. Jeremy Sharon, *State witness agreement with former Netanyahu aide Shlomo Filber to be annulled*, TIMES OF ISR. (Apr. 8, 2024), www.timesofisrael.com/state-witness-agreement-with-former-netanyahu-aide-shlomo-filber-to-be-annulled/.

198. *See, e.g.*, Ido Baum, לקראת החקירה הנגדית של פילבר. בסנגוריה בונים על "תיאוריית הצבירה" [*Ahead of Filber's Cross-Examination: The Defense Builds on the "Accumulation Theory"*], THE MARKER (Apr. 20, 2022), www.haaretz.co.il/law/2022-04-20/ty-article/.premium/00000180-6564-dc2a-a5ee-fd651a260000 (Isr.).

199. *See* Oren Persiko, המשטרה של כולנו [*The Police of the People*], THE SEVENTH EYE (Feb. 28, 2022), www.the7eye.org.il/448032 (Isr.).

200. Tova Zimoki, לוין הודיע: תוקם ועדת בדיקה ממשלתית לשימוש ברוגלות [*Levin: A Governmental Committee of Inquiry Regarding Spyware will be Established*], YNET (July 20, 2023), www.ynet.co.il/news/article/r1qrxru5n (Isr.).

201. Yehuda Shlezinger, השב"כ לראש הממשלה: מתנגדים לוועדת חקירה בעניין פגסוס [*Shin Bet to Prime Minister: We Oppose Another Committee of Inquiry Regarding Pegasus*], ISRAEL TODAY (Aug. 24, 2023), www.israelhayom.co.il/news/politics/article/14534166 (Isr.).

202. HCJ 6509/23 Argaman v. Prime Minister & Others, (2024) (Isr.), supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts%5C23/090/065/L15&fileName=23065090.L15&type=4.

203. *Id.*

issues directly related to Netanyahu's case.[204] As of September 2025, the Drori Committee is still in session.[205]

In parallel with the committee's activities, Netanyahu's coalition promoted legislation aimed at legalizing the use of spyware in severe crime investigations, with a notable exception: cases involving charges of bribery or corruption, such as those Netanyahu faces.[206] As of November 2024, the proposed legislation has passed its first vote and is advancing through the legislative process.[207] The bill has drawn significant criticism from multiple quarters. The Attorney General opposes the legislation due to the exclusion of corruption-related crimes.[208] Meanwhile, the Public Defender's Office has objected to the broader implications of legalizing spyware use, citing serious concerns about violations of privacy and the potential for abuse in remotely searching device contents.[209] The police have expressed strong support for the legislation, highlighting its potential utility in combating crime.[210]

B. *The European Union's PEGA Report*

The Pegasus Project and subsequent publications highlight the extensive use of Pegasus within the EU. It was reported that more than a thousand phone numbers on the Pegasus Project's "List" were

---

204. Netael Bendel, [*The Attorney General to the Supreme Court: The Spyware Committee of Inquiry Violates Your Directives*], ISR. TODAY (Mar. 11, 2024), www.israelhayom.co.il/news/law/article/15403296 (Isr.).

205. Press Release, Malware Investigative Committe [The Investigative Committee on Cyber Offensive Tools in Israeli Criminal Law Enforcement is Back in Session] (Feb. 22, 2024), www.gov.il/he/pages/resumption (Isr.).

206. *See* Tova Zimuki, [*The Attorney General Opposes Coalition's Bill: Demands Use of Spyware Also in Cases of Governmental Corruption*], YNET (Oct. 31, 2024), www.ynet.co.il/news/article/bjzx00nlbyx (Isr.).

207. Zvi Zerhia, [*The Spyware Law Passed the First Vote, But will Be Amended Before the Second*], CALCALIST (Nov. 13, 2024), www.calcalist.co.il/local_news/article/h1bwvbgg1x (Isr.).

208. Amiran Gil, [*Excluding Corruption Charges: The Bill that Will Allow the Police to Use Spyware Passed the Initial Vote in the Parliament*], GLOBES (Nov. 10, 2024), www.globes.co.il/news/article.aspx?did=1001493657 (Isr.).

209. *Id.*

210. Liran Tamari, [*Chief of Police to the Attorney General: Spyware Law is a Critical Tool for Us*], YNET (Nov. 18, 2024), www.ynet.co.il/news/article/sj8k8kuf1e (Isr.).

European numbers.[211] These reportedly included numerous senior figures, including the President of France, Emmanuel Macron.[212]

This does not mean, of course, that all the devices with European phone numbers targeted by the spyware were targeted by EU Member States. However, from the very beginning of the Pegasus revelations, the publications allege certain Member States bought the program and some of them abused it. For instance, during the initial days of the Pegasus Project, it was claimed that Hungary had used Pegasus to hack the phones of journalists, lawyers, and opposition leaders to suppress dissent in the country.[213]

This section reviews reports on the way Pegasus and similar programs have been employed in the EU. It then details the main findings of a designated committee that investigated these reports, reviews relevant EU legal and regulatory frameworks as they are presented in this report, and covers the aftermath of its publication.

1. Pegasus in the EU

By 2022, reports indicated that NSO had twenty-two clients in the EU, spread across fourteen of the Union's twenty-seven Member States.[214] Two of these clients had their contracts with NSO terminated by the company following investigations into abuse of the software.[215] While NSO disclosed some details to members of the European Parliament, it did not officially confirm the identity of the suspended clients.[216] Reports suggest, however, that these clients were Poland and Hungary.[217] These two countries were later found by EU entities to have used Pegasus for illegitimate purposes.[218] Nevertheless, this left at least twelve other EU jurisdictions actively using the spyware for reportedly more legitimate purposes, including Germany, the Netherlands,

211. Stephanie Kirchgaessner et al., *Revealed: leak uncovers global abuse of cyber-surveillance weapon*, THE GUARDIAN (July 18, 2021), www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

212. Angelique Chrisafis et al., *Emmanuel Macron identified in leaked Pegasus project data*, THE GUARDIAN (July 20, 2021), www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data.

213. Shaun Walker, *Viktor Orbán using NSO spyware in assault on media, data suggests*, THE GUARDIAN (July 18, 2021), www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests.

214. Since more than just one agency can gain access to the program in a certain country, there are cases in which NSO had more than one client in the same country; Benjakob, *supra* note 42.

215. PEGA report, *supra* note 108, ¶ 11.

216. Benjakob, *supra* note 42.

217. *See id.*

218. PEGA report, *supra* note 108, ¶¶ 79-80, 132-33.

and others.[219] In addition, other EU jurisdictions used similar surveillance products developed by other companies.[220]

The Pegasus revelations caused tension across Europe, both at the national level and within the Union's institutions themselves. This section does not delve into the specific actions and investigations undertaken by the national governments of individual EU Member States in response to the Pegasus Project. Instead, it briefly reviews the main conclusions reached by the European Parliament's designated investigative committee.

The Treaty on the European Union specifies that activities undertaken by Member States to protect their national security fall outside the scope of EU competence, meaning the legislation in the field is largely left to the Member States.[221] This exemption also applies to other EU legislative frameworks, including the General Data Protection Regulation (GDPR) and the Directive on Privacy and Electronic Communications.[222] However, a 2017 report by the European Union Agency for Fundamental Rights highlighted that the national security exemption "cannot be seen as entirely excluding applicability of EU law."[223]

Although Pegasus is often used in the context of national security, EU officials began reviewing its use within the Union. In September 2021, the EU Commissioner called for "urgent action" regarding Pegasus, initially framing the issue as "the responsibility of each and every member state."[224] In March 2022, the European Parliament decided to establish a special committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware within the EU. Known as the PEGA Committee, it prepared an extensive report and recommendations for the EU's institutions.[225] They were presented in May 2023.[226]

---

219. *Id.* ¶¶ 303-353, 354-359, 362-369.

220. Benjakob, *supra* note 42.

221. PEGA report, *supra* note 108, ¶ 8.

222. *See* European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services - Fundamental Rights Safeguards and Remedies in the EU - 2023 Update*, at 7 (May 24, 2023).

223. *Id.*

224. Daniel Boffey, *EU commissioner calls for urgent action against Pegasus spyware*, THE GUARDIAN (Sept. 15, 2021), www.theguardian.com/news/2021/sep/15/eu-poised-to-tighten-privacy-laws-after-pegasus-spyware-scandal.

225. PEGA report, *supra* note 108, ¶ 2.

226. *See generally id.*

2. The PEGA Report

The PEGA Report is a comprehensive document, issued by the investigative committee appointed at the European Parliament. It reviews various legal and policy aspects of Pegasus and similar spyware programs within the EU, including how different Member States used the spyware. It details how the program was abused in certain countries and mentions how it was used in others. Among other topics, the report examines the relevant legal frameworks in certain Member States and how they regulate the use of such technology in criminal justice and national security contexts.

a. Main Factual Findings

The PEGA Committee concluded that it "can be safely assumed that authorities in all member states use spyware in one way or another, some legitimate, some illegitimate."[227] It further found that, in the vast majority of Member States, the use of such programs by intelligence services is regulated by internal legal frameworks that include executive, parliamentary, and judicial review.[228] However, the committee noted that "concerns have been raised about certain countries' permissive intelligence frameworks, ineffective checks, lax oversight practices, and political interference."[229] Additionally, the report highlighted that spyware is also used by criminal law enforcement agencies, not only intelligence agencies, raising "serious concerns about the admissibility in court of such material as evidence in the context of EU police and justice cooperation."[230]

The report then examined which programs had been purchased by various Member States, the legal frameworks governing these purchases and practices, and whether those states complied with EU laws and regulations. While the report was prompted by the Pegasus scandal, it also reviewed other similar programs, such as Predator, developed by Intellexa.[231]

The PEGA committee investigated several Member States to analyze their use of spyware. Not all countries were cooperative.[232] The Polish government, for example, largely refused to engage with the committee's

227. *Id.* ¶ 10.
228. *Id.* ¶ 14.
229. *Id.*
230. *Id.* ¶¶ 14-16.
231. *See id.* ¶¶ 153-156.
232. *See id.* ¶ 17.

delegation and failed to answer questions.[233] Nevertheless, PEGA documented the use of Pegasus in Poland starting in 2017 or 2018, identifying targets that included opposition leaders and civil servants.[234] The committee concluded that Poland abused Pegasus and contextualized this abuse within the broader rule-of-law crisis in the country.[235]

Hungary faced similar criticisms. The committee found that Pegasus had been "grossly abused" in Hungary, with 300 individuals targeted, including lawyers, journalists, and political figures.[236] It noted that "political control over the use of surveillance in Hungary is complete."[237]

Greece was also criticized for insufficient mechanisms to regulate the use of Pegasus and similar programs.[238] The committee identified "patterns suggesting that the Greek government enables the use of spyware against journalists, politicians and businesspersons" and noted that "it also allows the export of spyware to countries with poor human rights records."[239]

Other countries were found to have some deficiencies in their responses to the Pegasus revelations but were presented in the report as having better safeguards against abuse. For example, Spain was identified as having "an independent justice system with sufficient safeguards," although "some questions remain" regarding how the Spanish government employed offensive cyber operations.[240] Cyprus, meanwhile, was noted to have "a robust legal framework for the protection of personal data and privacy."[241] Though there was no evidence presented to claim that Cyprus itself abused these programs, the report criticized how certain commercial spyware companies operated in Cyprus, observing that "in practice it would seem that rules are easy to circumvent and there are close ties between politicians, the security agencies, and the surveillance industry."[242]

As mentioned, several other EU jurisdictions used Pegasus and similar programs to monitor civilians. These jurisdictions were included in the report, which reviewed their legal frameworks. While their practices were not deemed abusive to the extent seen in countries like Poland

233. *Id.*
234. *Id.* ¶¶ 58-60.
235. *Id.* ¶¶ 79-80.
236. *Id.* ¶¶ 81-82.
237. *Id.* ¶ 106.
238. *Id.* ¶ 238.
239. *Id.*
240. *Id.* ¶ 350.
241. *Id.* ¶ 302.
242. *Id.*

and Hungary, the report's analysis of Germany's, Spain's, and the Netherlands' legal systems offers potential lessons for shaping the legal landscape in the United States. The following subsection draws on the comparative analysis presented in the PEGA Report to introduce anecdotes on the legal mechanisms employed by EU Member States to regulate cyber operations in criminal justice settings.

b. Notable EU Statutory Frameworks According to the PEGA Report

The PEGA Report uses several studies to substantiate its findings,[243] including a comparative analysis of the existing legal framework in various EU Member States for the use of Pegasus and equivalent software.[244] This study, and the PEGA Report itself, generally classify the legal measures aimed at regulating spyware like Pegasus into two broad categories: ex-ante and ex-post scrutiny. Ex-ante measures consist of laws and regulations designed to prevent unnecessary, offensive, or abusive infections before they occur. These measures include, first and foremost, requirements such as obtaining judicial warrants. Ex-post measures ensure that there are effective oversight mechanisms that assure infections have not been abused after they occurred. These mechanisms include informing the suspect that their device has been infected, reporting to a judge on the type of information obtained, or prosecuting individuals who have misused the spyware.

Both the PEGA Report and the comparative study that was submitted to the PEGA Committee discuss various anecdotes about oversight measures and preventive mechanisms employed by different EU jurisdictions to avoid the abusive use of tools like Pegasus. The examples presented here can provide valuable insights for U.S. policymakers considering regulatory frameworks for similar programs.

Germany is highlighted in the report as having a seemingly robust statutory framework relevant to this field.[245] The report emphasizes how Germany insisted, at a certain point, on acquiring only versions of spyware that were compliant with German law.[246] German law does allow authorities to obtain warrants to use these tools in a rather wide variety of criminal contexts. Since 2008, federal laws in Germany have

243. *See Spyware as a threat to fundamental rights and democracy in the EU*, EUR. PARL. (2024), www.europarl.europa.eu/RegData/etudes/BRIE/2024/761472/IPOL_BRI(2024)761472_EN.pdf [hereinafter *Spyware as a threat*].

244. *See generally* Quentin Liger & Mirja Gutheil, *The Use of Pegasus and Equivalent Surveillance Spyware: The Existing Legal Framework in EU Member States for the Acquisition and Use of Pegasus and Equivalent Surveillance Spyware,* EUR. PARL. (2023), www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.

245. *See* PEGA report, *supra* note 108, ¶¶ 363-64.

246. *See* Liger & Gutheil, *supra* note 244, at 20.

granted police the authority to use hacking powers in national security contexts, particularly to prevent terrorism.[247] The reports states that in 2017, a new law came into effect allowing all law enforcement agencies to use state-sponsored hacking tools for the investigation of forty-two specified criminal offenses.[248] These offenses include fraudulent asylum applications, tax evasion, and drug-related crimes, among others.[249] The report further notes that while these tools are often justified by stakeholders as being essential for combating serious crimes like child pornography, most investigations using spyware have focused on other types of crimes.[250]

For a warrant to be secured, a few conditions must be met. The requesting agency must demonstrate suspicion regarding an individual based on factual grounds; disclose such information as the identity and the location of the target; and disclose the type, extent, and duration of the requested measure.[251] Further, the comparative study presented to the PEGA Committee notes that "intercepted data concerning the core area of the private conduct of life is regarded as off-limits and inadmissible" under German law.[252]

German law draws a distinction between accessing live communication and accessing all stored information on a device.[253] Pegasus allows broader access, which German authorities found inconsistent with legal standards. Following a court decision, German authorities required NSO to modify Pegasus so that it would only allow access to live communications.[254] Initially, NSO resisted, but following negotiations, it provided a modified version.[255] German authorities implemented similar measures for other spyware tools, such as FinFisher, ensuring that these tools were deemed "technically clean" and fully compliant with governmental approvals before being put into use.[256]

As to ex-post measures, in criminal cases, the person affected by the interception of the search must be informed as soon as possible without endangering the investigation, persons involved, or significant assets.[257]

247. PEGA report, *supra* note 108, ¶ 363.
248. *Id.*
249. *Id.*
250. *Id.* ¶ 364.
251. Liger & Gutheil, *supra* note 244, at 58.
252. *Id.* at 59.
253. PEGA report, *supra* note 108, ¶ 365.
254. *Id.*
255. *Id.*
256. *Id.* ¶ 367.
257. Liger & Gutheil, *supra* note 244, at 59-61.

In cases of deferred notification, the decision to defer must be documented and approved by the court if that decision to defer goes beyond twelve months.[258] Reports on the use of these tools should be submitted annually by the relevant enforcement agencies.[259] The study also mentions other forms of oversight, including a parliamentary oversight panel.[260]

In the Netherlands, public prosecutors are required to obtain written authorization from an investigative judge to hack a device.[261] It can be extended beyond the period originally requested, and that judicial authorization could be "provided orally in urgent need, as long as the authorization for the extension is eventually provided in written form within three days."[262] The Central Review Commission, an administrative oversight mechanism, is required to provide advice to the investigative judge before it makes a decision.[263] Hacking warrants can only be issued for a maximum of four weeks, and extended by an additional period of four weeks at a time.[264] Warrants can only be approved toward the investigation of crimes for which the maximum sentence is four years in prison, except for specifically designated crimes with lower maximum sentence; crimes that are "serious breaches of law"; when "the investigation requires this urgently"; or in limited technical settings, such as when it is needed to establish certain characteristics of an automated device.[265]

As to the Dutch ex-post mechanisms, according to the comparative study presented to the PEGA Committee, they are based first and foremost on the assumption that when a case goes to trial, the court measures the evidence and the ways they were obtained.[266] The Computer Crime Act, for example, includes a provision foreseeing oversight, but the study paints this mechanism as vague.[267] The law in the Netherlands requires notifying the suspects that they have been hacked once the investigation is over.[268]

258. *Id.*
259. *See id.* at 60-61.
260. *See id.* at 61.
261. *Id.* at 66.
262. *Id.*
263. *Id.*
264. *Id.*
265. *Id.* at 67.
266. *Id.* at 68.
267. *See id.* at 66, 75.
268. *Id.*

Spain was found to have used Pegasus,[269] alongside other cybersurveillance programs,[270] and was criticized for it by the PEGA Committee—though much more mildly than others. While the committee identified deficiencies in Spain's regulation of spyware, it noted that "Spain has an independent justice system with sufficient safeguards."[271]

The Spanish Criminal Procedure Act permits privacy infringements, provided they are subject to judicial warrants.[272] The law also establishes a rigid judicial supervision mechanism that requires courts to oversee the implementation of surveillance measures. Judges authorizing surveillance must specify both the frequency and the form in which judicial police must report back on the progress and execution of the surveillance.[273] For an order to be granted, the request must include a description of the event under investigation, a detailed justification for the use of spyware, the scope of the measure being sought, a specification of its content, and the duration for which it is required.[274]

As to ex-post mechanisms, Spain has an ombudsperson—the Defensor del Pueblo—who is authorized to undertake inquiries on topics related to the field.[275] Spain also has an Official Secrets Committee in the Congress that offers parliamentary oversight.[276] The PEGA Report also lists several cases submitted to Spanish courts for the review of claims regarding spyware use over the past several years.[277]

In Greece, judicial authorization for monitoring private communications requires approval from the Public Prosecutor.[278] It could be allowed only "if [the investigation involves] a criminal act, there is serious suspicion of guilt, there are no alternative measures, and the use is limited in time."[279] However, a 2018 amendment made it easier to obtain warrants by reducing the number of prosecutors needed to authorize wiretapping.[280] The report describes mechanisms for parliamentary and administrative oversight of surveillance practices.[281]

269. PEGA report, *supra* note 108, ¶¶ 305-07.
270. *Id.* ¶¶ 308-09.
271. *Id.* ¶ 350.
272. *Id.* ¶¶ 310-12.
273. *Id.* ¶ 314.
274. Liger & Gutheil, *supra* note 244, at 50.
275. *Id.* at 51.
276. *Id.*
277. PEGA report, *supra* note 108, ¶¶ 326-28, 349.
278. *Id.* ¶ 168.
279. Liger & Gutheil, *supra* note 244, at 47.
280. PEGA report, *supra* note 108, ¶ 168.
281. *Id.* at 172-73.

The Greek legal system includes three main relevant oversight authorities.[282] The first authority is a non-parliamentary committee that is designated by the parliament and appointed by the Minister of Justice (ADAE).[283] The second authority is the Special Standing Committee for Institutions and Transparency, which is a parliamentary committee.[284] The Hellenic Data Protection Authority, the third authority, is tasked with ensuring the protection of communication confidentiality,[285] and is administratively independent.[286] Greek law allows confidentiality to be waived only in cases of national security or serious crimes.[287] However, the PEGA Report criticizes a 2022 amendment that weakened these protections.[288] It noted that the new oversight mechanism overseeing surveillance requests is dominated by those responsible for initiating and authorizing surveillance, thereby undermining independent review.[289]

At the EU level, the report identifies several legislative frameworks that could serve as regulatory tools for spyware.[290] These include data and privacy protection measures such as the GDPR.[291] However, the report finds that the enforcement of such frameworks has been relatively weak.[292]

The PEGA Report concludes that the EU, as an institution, lacks the capacity to respond effectively when Member States abuse spyware.[293] While the use of spyware was found to "pose threats to democracy, the rule of law, and the fundamental rights of individual citizens," the report also found that "[t]he EU has few powers to act on these threats, and it turns out to be ill-equipped against potential criminal activity by national authorities, even if it affects the EU itself."[294] Although the report acknowledged the establishment of the PEGA Committee itself, as well as other actions taken by the EU, it also noted that these measures are of limited effect.[295]

---

282. Liger & Gutheil, *supra* note 244, at 49.
283. *Id.*
284. *Id.*
285. PEGA report, *supra* note 108, ¶¶ 172-73.
286. *Id.*
287. *Id.* ¶ 174.
288. *Id.* ¶ 176.
289. *Id.*
290. *Id.* ¶ 519.
291. *Id.*
292. *Id.*
293. *See id.* ¶ 515.
294. *Id.*
295. *Id.* ¶¶ 517-18.

3. EU Parliamentary Recommendation

Based on the findings of the PEGA report, a draft recommendation for the Union's institutions has been presented. The draft recommendation "strongly [condemns] the use of spyware by Member State governments … for the purpose of monitoring, blackmailing, intimidating, manipulating, and discrediting opposition members, critics and civil society, eliminating democratic security and the free press."[296] It further concludes that there is evidence of "degrees and forms of contravention and maladministration of EU law in Poland, Hungary, and Greece."[297]

The recommendation to the Commission, which was adopted by the European Parliament in 2023, "highlights the undeniable importance" of concepts such as privacy and explicitly condemns the use of spyware for illegitimate purposes, including blackmailing, intimidation, and manipulation.[298] It uses similarly strong language to express dissatisfaction with various findings from the PEGA Report.[299] It also calls on specific countries—particularly Poland, Hungary, Greece, Cyprus, and Spain—to implement stronger oversight mechanisms and initiate investigations into the abuse of Pegasus and similar products within their jurisdictions.[300] Furthermore, the recommendation emphasizes the broader "need for boundaries to national security" and advocates for the "better implementation and enforcement of existing legislation."[301] It suggests setting up a special task force focusing on elections, a tech lab, implementing a rule of law toolbox, and coming forward with legislative proposals.[302]

The effectiveness of these statements could be debated. In fact, the PEGA Report itself acknowledges the limited powers available to EU institutions in this area.[303] The EU generally lacks authority to act in matters of national security, as these remain primarily under the

296. *Investigation of the Use of Pegasus and Equivalent Surveillance Spyware*, ¶ 3, 2024 O.J. (C 494) 1, www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html [hereinafter European Parliament Recommendation].

297. Dumbrava, *supra* note 46, *see also* European Parliament Recommendation, supra note 296, ¶¶ 14, 17, 19.

298. European Parliament Recommendation, *supra* note 296, ¶¶ 1, 3 ("Strongly condemns the use of spyware by Member State governments […] for the purpose of monitoring, blackmailing, intimidating […] points out that this illegitimate use of spyware […] affects the Union's institutions").

299. *See id.*

300. *See id.* ¶¶ 15-24.

301. *See id.* ¶¶ 42-66.

302. *See Spyware as a threat*, *supra* note 243.

303. PEGA report, *supra* note 108, ¶ 516.

sovereignty of Member States.[304] Similarly, the EU's judiciary has limited capacity to address such issues, as its proceedings are often lengthy and its ability to provide concrete remedies to petitioners is constrained.[305] Despite these limitations, the report emphasizes that national security should not be interpreted as an unlimited exemption from compliance with EU laws and treaties, and at least reveals how widely these programs are used in EU Member States, including many liberal democracies.

Furthermore, reports emerged in 2024 that two additional members of the European Parliament and one staffer had been infected with Pegasus.[306] Figures in civil society then urged the EU Council and Commission to revisit the PEGA Committee's findings and take meaningful steps to address the issues raised.[307]

C. *Lessons from Beyond Seas*

What lessons could U.S. stakeholders potentially learn, or at least use as an initial line for debate, using a comparative perspective? The Israeli and European examples differ in many ways. The Merari Report and the PEGA Report also differ significantly in their goals and perspectives. Nonetheless, both provide valuable lessons about the challenges and opportunities that spyware like Pegasus presents to democratic nations in the context of criminal enforcement. There may be meaningful insights to be gained from their experiences when shaping U.S. policies in the field.

First, and most fundamentally, both Israel and the EU faced the need to determine how these programs were being used and whether they complied with domestic laws only after journalistic investigations revealed the ways in which these tools were employed. Even when no extremely abusive practices were initially uncovered, legal questions and dilemmas were found to have been inadequately addressed in advance. A critical takeaway is the importance of defining in advance what these programs should and should not do in the domestic legal landscape before deploying them in a criminal setting, particularly on a

304. *Id.* ¶ 8.

305. *Id.* ¶ 529.

306. Antoaneta Roussi, *Brussels spyware crisis expands: Two MEPs hit in phone-hacking security breach*, POLITICO (Feb. 22, 2024), www.politico.eu/article/nathalie-loiseau-elena-yoncheva-pegasus-spyware-european-parliament-security-defense-subcommittee/.

307. *See,* e.g., Silvia Lorenzo Perez, *EU Council and EU Commission Must Urgently Address Issues by PEGA Committee*, CTR. FOR DEMOCRACY & TECH. (Mar. 7, 2024), www.cdt.org/insights/eu-council-and-eu-commission-must-urgently-address-issues-by-pega-committee/.

large scale. The United States has an opportunity to take proactive steps in this regard. Establishing clear policies early on can prevent abusive practices, avert political instability, and minimize embarrassment later.

Second, it is essential that law enforcement agencies in democratic countries only gain access to programs whose capabilities are strictly limited to what is permissible under domestic law. Both the Israeli and German examples demonstrate the potential to negotiate with software firms to secure modified versions of tools that align with local legal restrictions. For instance, if the law allows only the interception of live communications and prohibits accessing stored content, Pegasus must be configured to access live communications exclusively. Ensuring this alignment between technological capabilities and legal constraints is crucial and should ideally be done in advance.

Third, to achieve this goal, it is critical to clarify which aspects of existing criminal procedural rules apply to these tools and what those rules authorize. This avoids the situation where unresolved legal debates remain unaddressed before the program is deployed. For instance, it must be determined whether specific functions within tools like Pegasus—such as automatically generating a list of installed applications—constitute wiretapping or searching. These distinctions are not always straightforward and require comprehensive legal analysis within each jurisdiction based on domestic law. Answering these questions in advance helps prevent violations of suspects' rights. In cases where existing laws governing wiretapping and searches are insufficient, new legislation should be considered.

Fourth, for ex-ante mechanisms to be effective, it is imperative to ensure that judges and prosecutors fully understand what it is exactly that they are authorizing. This can be achieved by providing education on the methods and capabilities of tools like Pegasus and ensuring that all relevant documentation clearly and thoroughly explains the nature of the search or wiretap being requested, as the Merari Report suggested.

These lessons may appear broad and somewhat vague, but they provide a useful framework for evaluating the current U.S. legal landscape. The following parts will introduce existing U.S. constitutional and statutory doctrines and assess how they might apply to cybersurveillance tools like Pegasus. The Article will then identify potential gaps and present broader recommendations, including proposals for new administrative policies and, where necessary, revisions to existing legal frameworks informed by the comparative lessons.

IV. Commercial Spyware and the Fourth Amendment

"Time works change," noted Justice Brandeis in his dissenting opinion in *Olmstead v. United States*.[308] "[It] brings into existence new conditions and purposes. Therefore, a principle, to be vital, must be capable of wider application than the mischief which gave it birth."[309] Technological advancement brings new legal challenges. Over the years, scholars have observed that new technological inventions pose novel legal questions, time and time again, forcing the courts to reevaluate their approach toward the Fourth Amendment. These include tracking technologies, drones, cell site simulators, and more.[310]

Surveillance technologies are developing at a remarkably rapid pace, and courts are accordingly confronted with the necessity to address their advancement. The result is a diverse selection of doctrines that do not always agree with one another as to the articulation and operation of the Fourth Amendment in this modern age of surveillance.[311] This part first shortly introduces the Fourth Amendment and its interpretation in light of modern surveillance technologies. It then argues that spyware like Pegasus should be understood as a "search" under the Fourth Amendment, initiating at the time of the infection.

A. *A Brief Introduction to the Fourth Amendment and Modern Surveillance*

The Fourth Amendment consists of two clauses. The Reasonableness Clause protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[312] The Warrant Clause defines when and how search warrants may be issued, and requires "probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[313] The relationship between the two clauses has been subject to research and debate. While some claim that the two clauses are ultimately distinct, others argue that the second helps to explain the first.[314]

Initially, the Fourth Amendment was a response to controversies surrounding general warrants issued by the British in the former colonies.[315]

---

308. Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

309. *Id.*

310. *See* David Gray, The Fourth Amendment in the Age of Surveillance 23-33 (2017).

311. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv. L. Rev. 757, 802-03 (1994).

312. U.S. Const. amend. IV.

313. *Id.*

314. *See* Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 Am. Crim. L. Rev. 1389, 1389-90 (1989).

315. *See* Gray, *supra* note 310, at 142.

Over the century following its ratification, the Fourth Amendment received limited judicial attention, among other reasons, due to the rather limited scope of organized law enforcement at the time.[316] The Fourth Amendment began attracting the attention of the Supreme Court of the United States more widely when law enforcement agencies became more prominent, especially around the late nineteenth and early twentieth centuries.[317] In *Boyd v. United States* (1886), the Supreme Court found that forcing a suspect to produce papers during an investigation qualifies as a "search" under the Fourth Amendment.[318] The case exemplifies how, in its early days, the Fourth Amendment was understood as linked to property rights and mirrored the common law of trespass in a physical manner.[319]

As technology developed, the Court was faced with new legal challenges and was compelled to develop new doctrines to address them. In *Olmstead v. United States* (1928), the Court faced new wiretapping technology, installed manually on a suspect's telephone lines.[320] Writing for the Court, Justice Taft found the practice to be lawful and constitutional under the Fourth Amendment, as the agents never trespassed on the suspects' property while installing the wires.[321] The term "search," the Court found, referred to "physical" invasion or seizure.[322]

The Court had a different understanding of the term "search" in *Katz v. United States* (1967).[323] The case concerned a suspect who allegedly transmitted gambling information using a public phone booth. Law enforcement officers recorded these conversations without a warrant.[324] The Supreme Court, in response, developed the Reasonable Expectation of Privacy Doctrine, aimed at determining whether a person's privacy has been illegitimately violated.[325] Indeed, focusing on the physical element of the term "search" could have easily resulted in the conclusion that Katz was never searched. The police never entered his premises nor physically searched any of his belongings. Justice Harlan noted, "[In the] enclosed telephone booth . . . a person has a constitutionally protected reasonable expectation of privacy . . . . The

316. *Id.* at 72.
317. *See id.*
318. *See* Boyd v. United States, 116 U.S. 616 (1886).
319. GRAY, *supra* note 310, at 72.
320. *See* Olmstead v. United States, 277 U.S. 438, 456-57 (1928).
321. *See id.* at 465-66.
322. *Id.*
323. Katz v. United States, 389 U.S. 347 (1967).
324. *Id.* at 348-49.
325. *See id.* at 360.

electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment".[326]

The Court had to develop different legal presumptions to address emerging Fourth Amendment dilemmas, given the vagueness of the Reasonable Expectation of Privacy Doctrine.[327] Among the interpretational tools developed is the Third-Party Doctrine, as demonstrated in *United States v. Miller* (1976),[328] and *Smith v. Maryland* (1979).[329] In *Miller*, the state subpoenaed the defendant's bank account documentation and used it as evidence in his trial.[330] The Court found the documents not to be Miller's protected private information, but rather the bank's records.[331] The bank, as a third party, could have handed these documents to the government.[332] In *Smith*, the Court found that a telephone company is a third party and that accordingly, the registry of the numbers dialed by the defendant had been handed to a third party, making them unprotected by the Fourth Amendment.[333]

The opinion of the Court in *United States v. Jones* (2012) signals yet again an approach focusing on the physical intrusion aspect of what constitutes a "search."[334] The case concerned the constitutionality of tracking a suspect's car by attaching a GPS device to it.[335] The Court found that attaching the tracking device to a car without a warrant violates the Fourth Amendment.[336] However, in this case, the majority focused mostly on the physical aspect of the practice rather than on the vaguer *Katz* standard of legitimate expectation of privacy.[337] The *Katz* standard in this case is irrelevant, Justice Scalia ruled, because the case does not fall within the *Katz* formulation.[338] *Katz* does not withdraw any protection that the literal meaning of the Fourth Amendment extends to, like physical intrusion of property.[339]

---

326. *Id.* at 388-89.

327. *See* Matthew Tokson & Paul Ohm, *Carpenter Should Replace Katz in Fourth Amendment Law*, LAWFARE (July 13, 2022), www.lawfaremedia.org/article/carpenter-should-replace-katz-fourth-amendment-law.

328. United States v. Miller, 425 U.S. 435 (1976).

329. Smith v. Maryland, 442 U.S. 735 (1979).

330. *Miller*, 425 U.S. at 438-39.

331. *Id.* at 444-45.

332. *Id.*

333. *See Smith*, 442 U.S. at 745-46.

334. United States v. Jones, 565 U.S. 400 (2012).

335. *Id.* at 402.

336. *Id.* at 404-05.

337. *See id.*

338. *Id.* at 406.

339. *See id.* at 407.

The defendant in *Riley v. California* (2014) was searched following defects found with his car registration.[340] During the search, two guns were found in the car, and he was arrested.[341] His phone was searched, revealing his connections with a street gang.[342] The Court found that the warrantless search violated Riley's Fourth Amendment rights.[343] The Court focused on the unique characteristics of cellphones in modern days and pointed out that the fact that technology allows a person to carry his most sensitive documents in his belongings all the time should not make his Fourth Amendment rights any less protected.[344]

More recently, in *Carpenter v. United States* (2017), the Court once again developed a new variation of the Reasonable Expectation of Privacy Doctrine.[345] The case concerned obtaining location information using Cell Site Location Information (CSLI).[346] The Court found that the warrantless acquisition of the CSLI records breached Fourth Amendment rights.[347] The Third-Party Doctrine does not apply, the Court found, due to the difference between the "limited types" of personal information addressed in *Smith* and *Miller*, and the exhaustive chronicle of location information collected by wireless carriers and disclosed to the government in *Carpenter*.[348]

In this regard, *Carpenter* can be interpreted as supportive of the "mosaic approach" to the Fourth Amendment. This theory focuses on the collective sequence of all governmental investigative activity instead of on each step of an investigation individually, so the sequence could amount to a search.[349] The question is not whether every particular action is offensive or intrusive enough to be perceived as a search under the Fourth Amendment, but rather the "mosaic," the puzzle the government would be able to assemble regarding a person's life, counting all the investigative efforts combined.[350] In *Carpenter*, the Court mentioned at least three factors to be considered within its de facto updated doctrine or test of privacy expectation breach: it stressed how deeply revealing the kind of data obtained by the government is, as it "provides

340. Riley v. California, 573 U.S. 373, 378 (2014).
341. *Id.*
342. *Id.* at 379-80.
343. *Id.* at 403.
344. *See id.* at 396-97.
345. *See* Carpenter v. United States, 585 U.S. 296 (2018).
346. *Id.* at 300-01.
347. *Id.* at 316-17.
348. *Id.* at 313-14.
349. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012).
350. *See id.* at 328.

an intimate window into a person's life;"[351] it considered the large amount of data collected;[352] and noted that the information was not handed to the third party, the cellular carrier, voluntarily.[353]

Over the years, then, the Supreme Court has struggled with defining the breadth of Fourth Amendment protections, especially when faced with emerging surveillance technologies. In some cases, it focused mostly on physical property and trespass; in others, it focused on the target's legitimate expectation of privacy. Even when the test considered mostly the existence of the expectation of privacy, the vagueness of *Katz*'s test led the Court to develop sub-doctrines to make it applicable. Among these are the Third-Party Doctrine and the considerations mentioned in *Carpenter*. The application of these different legal doctrines is often far from coherent and may cause confusion and undermine legal certainty.[354] In reality, some have argued, the *Katz* doctrine is deeply rooted in the law, but at the same time, the more concrete test suggested in *Carpenter* is also being used regularly and increasingly.[355]

The Fourth Amendment seems to be at a turning point. Recent technological developments could lead to a situation where current doctrinal ambiguity is likely to only deepen.[356] Given the growing implementation of spyware as a method of law enforcement globally, and evidence that the United States is interested in using these technologies as well, it is crucial to consider the implications of these technologies in the U.S. context.

B. *Why and When Should Commercial Spyware Use Qualify as Searches*

As mentioned, Pegasus and similar tools could be viewed as more of a toolbox rather than one unified tool. This section analyzes different abilities presented by these programs and their interaction with Fourth Amendment interpretation. It first reviews capabilities classified as searching the infected device itself and then discusses those involving searching the surroundings of the device, using the device. Finally, this section discusses at what point the "search" begins and argues it begins with the infection itself.

---

351. *See Carpenter*, 585 U.S. at 311.

352. *Id.* at 314.

353. *Id.* at 315.

354. *See* Tokson & Ohm, *supra* note 327.

355. *See id.*

356. *See* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1851 (2022).

1. Searching a Device

Pegasus presents advanced surveillance features, but state hacking is not a new phenomenon. U.S. federal courts have previously grappled with the legal complexities arising from state surveillance. As the literature acknowledges, the most challenging cases often involve remote access to data.[357] It has been suggested that a superior rule under the Fourth Amendment should hold that any infringement on the logical integrity of metadata constitutes a search.[358] Emerging technologies like Pegasus introduce questions regarding how and when this rule applies, given the fact that such technologies access metadata remotely. They also present complexities in determining the precise moment a search begins, given their zero-click abilities. In other words, instinctively, it seems implausible to seriously claim that Pegasus is *not* conducting a search. But why? I argue that employing Pegasus to search a device and its contents can be analyzed through at least two legal doctrines.

The first, and perhaps more obvious route under current legal doctrine, would focus on the Reasonable Expectation of Privacy Doctrine, noting *Katz* and *Carpenter*. The second option would be to analyze Pegasus as a form of trespass under doctrines closer to *Jones* and the more traditional common law approach.[359] Both routes lead to the inevitable conclusion that infecting a phone with Pegasus is indeed a search under the Fourth Amendment, but I argue that the second route is a more favorable and analytically accurate interpretation.

As I reviewed, modern Supreme Court decisions analyzing the Fourth Amendment have focused mostly on the Reasonable Expectation of Privacy Doctrine. There are gaps between the way it was analyzed in *Katz*, where the doctrine was coined, and in *Carpenter*, which uses a more mosaic approach to the Fourth Amendment.[360] Regardless, it seems as if these two approaches to a similar doctrine acknowledge that the Fourth Amendment only protects individuals from unwarranted searches if they have reasonable expectations of privacy.

---

357. Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 596 (2018).

358. *Id.* at 609.

359. *See* SARA E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA, 19-21 (Harv. Univ. Press 2018) ("Officially, the law of trespass and unreasonable search and seizure ruled, following the Anglo-American legal tradition in which the house and home were associated with 'security against violent invasion.'").

360. *See* Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507 (2023); Tokson & Ohm, *supra* note 327.

Katz first introduced the Reasonable Expectation of Privacy Doctrine.[361] It only protects individuals from unwarranted searches if they have such reasonable expectations. In later cases, trying to make the doctrine more broadly applicable, the Court developed the Third-Party Doctrine.[362] The classic application of the doctrine is not relevant here *per se*. Pegasus does not obtain the information through any third party but rather by invading the user's device itself. The Third-Party Doctrine could, however, be used to try and estimate what level of reasonable expectation we can define when dealing with targets of this technology. If a person does not have a reasonable expectation of privacy given that the information being searched was shared with a third party, we should consider what information Pegasus has access to that is shared by the user with a third party. Some information can be saved on a device and not shared with anyone. Other forms of content, however, are shared with third parties. Does it imply anything about the reasonable expectation of privacy regarding such content?

First, the content is often encrypted. Meta, for instance, cannot access messages sent on WhatsApp.[363] Even if Meta had such access, or if such information was shared with them directly by the user, allowing access to that information based on the Third-Party Doctrine seems weak given that the Supreme Court noted in *Riley* that cellphones require unique protection.[364] *Carpenter* further stressed that CSLI cannot be accessed without a warrant issued based on probable cause, pursuant to the quality of the intimate window the information obtained through CSLI opens into a person's life; the amount of data that could be collected; and that the information is not handed to the third party voluntarily.[365] In the equivalent situation, conducting a similar kind of surveillance using Pegasus, I argue, should then require a warrant.

As to the quantity and quality of the data the government may gather through these programs, the *Carpenter* test supports the claim that using Pegasus and equivalent programs qualifies as a search. The tricky questions regarding the application of the *Carpenter* test to a Pegasus infection surround the third factor: whether the information was voluntarily disclosed to a third party. In this regard, one may argue that a large

361. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

362. *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976) (noting that the general expectation of privacy test had to be examined through the lenses of the third party doctrine in both cases).

363. *See* WhatsApp Help Center, *supra* note 105 ("End-to-end encryption means that messages are encrypted to protect against WhatsApp and third parties from reading them.").

364. *See* Riley v. California, 573 U.S. 373, 403 (2014).

365. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018).

portion of the information being accessed by Pegasus is actually handed to a third party voluntarily, or at least at a much more voluntary level compared to CSLI information. Users cannot opt out of CSLI services if they use a functioning phone. That is not the case with features like geolocation that can be rather easily shut down by the users using their smartphone. In fact, Google is apparently troubled by the fact it has access to geolocation data and is gradually changing the service to ensure that data is only accessible through the device itself.[366]

Under the *Carpenter* doctrine, whether and how the service provider can access the content matters, especially given that the *Carpenter* majority went out of its way to highlight that its decision is narrow. The Court stated,

> [The Carpenter decision] is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' . . . . We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques . . . [O]ur opinion does not consider other collection techniques involving foreign affairs or national security.[367]

It is beneficial to reevaluate the third *Carpenter* factor given these new technologies. In this regard, a test focused on checking whether the data has been shared voluntarily, seems outdated. The test could focus, instead, on whether the data has been shared to allow the user to have access to a service that is an essential part of modern social life—email, social media, and navigation, for instance—and to which there is no viable alternative.

It also makes sense to clarify whether it matters if the information that was shared with a third party is obtained through said third party (as was the case in *Carpenter*, *Miller*, and *Smith*) or not. In the event the information was actually obtained through a third party, questions regarding the essentiality of that service, or whether the information or data was handed to that service provider voluntarily, could emerge. But this entire discussion seems largely irrelevant when the information—whether it was or was not voluntarily disclosed to a third party—was not obtained through that third party, but rather through hacking. The claim that obtaining information is not a search becomes much weaker if the information was not obtained through a third party. If the third

366. *See* Chris Velazco, *Google is rolling out new protections for our location data*, WASH. POST (Dec. 14, 2023), www.washingtonpost.com/technology/2023/12/14/google-maps-location-history/.

367. *Carpenter*, 585 U.S. 296 at 316.

factor mentioned in *Carpenter* could only apply toward situations in which the data was disclosed by the third party, then using Pegasus to obtain access to data on a suspect's phone would qualify as a search, simply because it typically does not involve the third party. In other words, whether information was disclosed to third parties—such as WhatsApp—should be legally irrelevant, if the information was eventually obtained through hacking and not through WhatsApp itself. There is little doubt, of course, regarding the other factors mentioned in *Carpenter* in the typical Pegasus infection case.

This route is coherent with an approach to the Fourth Amendment that focuses on the content that is being searched, rather than on the method or the actions taken to allow that search. In using spyware such as Pegasus, however, this method may not suffice in some scenarios.

Let us imagine that the government infects a phone. The only thing that is being viewed through the infected device is the user's public Twitter profile. The operator infects the phone, launches Twitter, goes directly to the user's public profile, reads it thoroughly, and then logs out without ever inspecting the device's contents again. In theory, the information obtained through this procedure could have been obtained by simply looking at the user's public Twitter profile from any computer—no infection was needed. Does that mean that the whole infection procedure, the active usage of Pegasus or a similar program, was not a search?

This is an extreme example, but one can imagine similar scenarios that raise similar questions. For instance, what if the police infected a phone, then launched the camera remotely, only to find out that it has been covered by physical duct tape so that they cannot see anything? What if the police used Pegasus to obtain a WhatsApp correspondence, only to discover they have already obtained the exact same correspondence because it was voluntarily handed to them by the recipient of the message? Does it mean that trying to infect a phone with Pegasus and failing is not a search?[368] Instinctively, it seems unjust and dangerous to focus exclusively on the type of content being searched. A person's privacy is affected by the *infection*, even if later the *information* obtained is deemed useless or even nonexistent. What could explain that notion? Perhaps, the infection itself. Or, as it was called thus far in the common law tradition, the problem is *trespass*.

368. *See, e.g.*, *India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists*, AMNESTY INT'L (Dec. 28, 2023), www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

I argue that using Pegasus is in fact often closer to breaking into one's living room than wiretapping their phone. Using Pegasus entails a violation of property rights, a component of trespass, rather than a violation of mere expectation of privacy. Accordingly, the Third-Party Doctrine is largely irrelevant, much like the question of whether the information was or was not shared with that third party voluntarily. Pegasus does not ask Google, Meta, or Apple to share the data, nor does it break their encryption of the information. Instead, it gains access to that information via the user. It breaks into their private cyberspace and gains access to whatever the user himself can access.

If we take the metaphor of cyberspace as a place seriously, then cyberspace is as much of a private space as any physical space, and therefore it should be constitutionally protected. Courts have already used the metaphor of cyberspace as a place,[369] as space and cyberspace share at least *some* fundamental characteristics.[370] If cyberspace is a place, or at least close enough to be a space legally in this context, then Pegasus intrudes into a private space. It commits an act of *cybertrespass*. Actions of cybertrespass are criminal offenses when committed by individuals.[371] They should be taken equally seriously when conducted by the government.

To put it differently, a police officer once had to break into one's house to see someone's photo albums. The fact that today photos are accessible on phones does not make them any less protected.[372] In *Riley*, officers had physical access to the phone, but the fact that modern technologies allow access to these records remotely does not make that intrusion less intrusive.[373] Accordingly, intrusion into that space constitutes a search based on the physical reading of the Fourth Amendment, inspired by cases like *Olmstead,*[374] and more recently, *Jones.*[375]

Jones, in this regard, is of special importance. Justice Scalia focused there on the physical aspect of an intrusion. As he explained,

---

369. *See e.g.*, United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010). *See also* Mayer, *supra* note 357, at 610.

370. *See* Yehuda Kalay & John Marx, *Changing the Metaphor: Cyberspace as a Place*, *in* DIGITAL DESIGN: RESEARCH AND PRACTICE 20 (2003), *see also* David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV., 1367, 1379 (1996). *See generally* Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521 (2003).

371. *See* Michael J. O'Connor, *The Common Law of Cyber-Trespass*, 85 BROOK. L. REV. 421, 422, 426 (2020).

372. *See* Riley v. California, 573 U.S. 373, 393-396 (2013).

373. *See id.*

374. *See* Olmstead v. United States, 277 U.S. 438, 466-67 (1928).

375. *See* United States v. Jones, 565 U.S. 400, 404-05 (2012).

> [For] most of our history, the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas . . . it enumerates. Katz did not repudiate that understanding. . . . Katz . . . established that "property rights are not the sole measure of Fourth Amendment violations" but did not snuff out the previously recognized protection for property.[376]

Arguably, the Fourth Amendment test focusing on physical intrusion is perceived to be more conservative and could often lead to a weaker protection. However, in this case, perhaps counterintuitively, it in fact imposes *stricter* Fourth Amendment regulation toward the government. It means that the very infection itself, unrelated to whether private information was or was not obtained, is a search.

What Pegasus does is much closer to physical intrusion into a private space than violating a vaguer expectation of privacy. This intrusion happens even if the program only gains access to information in which the user does not have any expectation of privacy. When individuals hack another person's phone, their actions are considered criminal. Essentially, the government—when using these tools—does the same. The favorable legal framework to address Pegasus and similar programs is as a trespass—an intrusion into a private space that results in a search. Viewing these programs through these lenses leads to the conclusion that any form of Pegasus infection, no matter if and what information was obtained, is a search under the Fourth Amendment.

2. Searching the Surroundings Using a Device

The spyware can search beyond the contents of the device itself. It can launch the camera and microphone of a device remotely, without the consent or knowledge of the user. This set of capabilities, I argue, is not a search of the device. Rather, it is a search of everything surrounding the device, using the device. The police do not obtain any personal information that was created by the targets. Instead, it creates material that the user never saw and will never see. This capability should not be analyzed purely in terms of *cyber*surveillance. It is actually a form of *physical* surveillance, closer to bugging—a practice in which a surveillance tool is inserted or installed in a certain physical space—than wiretapping.

The fact that the police do not install any physical device, but instead remotely take over an existing device, should not matter: the intrusion

376. *Id.* at 406.

is nonetheless physical. In fact, it could be even more intrusive, because unlike ordinary surveillance devices used by law enforcement agencies, such as *Jones*'s tracker on a car, or a hidden camera in a room, phones travel with the target almost anywhere (in one survey, sixty-five percent of users admitted they use their phones in the restroom).[377]

Accordingly, this entire category of features constitutes a search, not of cyberspace but rather of the physical space in which the device is present. This may have some interesting implications for the way these tools can be used in practice. For example, since Pegasus can access the location of a phone, perhaps courts can allow law enforcement agencies to use a version of the spyware that will only be able to activate the camera in public locations, or in specific rooms or buildings that can be proven to be connected to any alleged crime, while not recording anything when the user is in more private spaces.

3. When Does the Search Begin?

The question of *whether* Pegasus infections constitute a search is distinct from determining *when* using spyware constitutes a search. Two main options can be considered when determining at what point the search begins. The first focuses on the contents accessed by Pegasus and may conclude that the search occurs when the data has been accessed. The second focuses on the intrusive nature of the program and may conclude that the search begins with the infection, even before any information has been accessed.

I argue that the program conducts a search at the moment of infection, even before any content has been accessed by the operator. This finding could be significant in practice: it means that the police cannot massively infect devices and then obtain warrants to access the information in retrospect, after the infection. This distinction could be crucial considering that some commercial spyware firms market their products by highlighting they can offer an unlimited scale of infections, up to twenty-five devices at a time.[378] Requiring a warrant at the moment of infection, rather than at the moment of accessing the content, could prevent potential abuse.

As discussed in Section IV.A, the Fourth Amendment is aimed at protecting a person's private space from governmental intrusion. If a person's personal cyberspace is protected as a physical space, then the

377. Mikhail Klimentov, *We all use phones on the toilet. Just don't sit more than 10 minutes.*, WASH. POST (Nov. 29, 2022), www.washingtonpost.com/video-games/2022/11/29/sitting-toilet-10-minutes-phone-nintendo-switch/.

378. PEGA report, *supra* note 108, ¶¶ 498-501.

intrusion of this space should qualify as the beginning of a search under the Fourth Amendment and should therefore be warranted. Or, to use Jonathan Mayer's language, if state hacking is a search under the Fourth Amendment because it "breaches the logical integrity of an electronic device," then with Pegasus-style spyware, that breach, that "exploitation," happens at the moment of infection.[379]

This analysis is not only analytically cleaner but also favorable from a policy standpoint. It would require law enforcement agencies to only infect devices they have reasonable cause to infect, preventing them from infecting large numbers of devices unjustifiably. Because the infection itself is intrusive, even before any content is obtained by the police, it is appropriate to treat the infection as the beginning of the search.

Lastly, it is worth noting that there might be a difference between different techniques of infection. In certain situations, especially when the infection is done using a zero-click mechanism, the question as to when the search begins might be irrelevant in practice. For example, in some cases, immediate usage of at least one of the surveillance program's features may be triggered at the moment of infection, for instance, if the program would automatically remove files to disguise the infection.[380] However, in other forms of infection, files may not necessarily be deleted. In these cases, it is justified to view the very infection itself as the beginning of a search, equivalent to breaking into one's private physical space.

V. Commercial Spyware in U.S. Statutory Practice

Pegasus and similar spywares possess a range of capabilities that have been broadly categorized into three main categories in this Article: accessing live data as it is being created; retrieving stored data; and generating new data—such as recording audio or video—using the infected device. Section V.A provides an initial review of how existing U.S. statutory frameworks may apply to each of these categories of spyware functionality, following that sequence.

Section V.B then examines potential actions that could be taken within the bounds of current legal frameworks through interpretation, identifies the limitations of these frameworks, and points out potential legal reforms to address gaps and ambiguities in the regulation of these tools. Specifically, this section mentions that the Wiretap Statute seems to permit the interception of live communications but does not cover

379. Mayer, *supra* note 357, at 628.

380. O'Cearbhaill & Marczak, *supra* note 98.

other forms of live content beyond communication. To distinguish between communications accessible under the Wiretap Statute and non-natural communicative content that should remain inaccessible, the section introduces the concept of a natural communication test.

A. *Navigating Existing Legal Frameworks for Cybersurveillance*

When considering the potential use of commercial spyware in U.S. criminal law enforcement, several existing legal frameworks come to mind. It appears that law enforcement officers interested in obtaining warrants to access electronic evidence could consider, today, in addition to the Fourth Amendment itself, the Federal Rules of Criminal Procedure; the All Writs Act; and the different sections of the Electronic Communications Privacy Act (ECPA).[381]

The Fourth Amendment establishes the foundational principle that government searches and seizures require a warrant based on probable cause.[382] Rule 41 of the Federal Rules of Criminal Procedure details the procedures for issuing such warrants, particularly for electronically stored information and tracking devices.[383] The All Writs Act of 1789 is a generalist piece of legislation, granting courts the authority to issue writs necessary to support their jurisdiction.[384] It has been used to attempt to compel tech companies to assist law enforcement in accessing electronic devices, though these efforts have faced legal challenges.[385]

The primary legislation governing the interception and access to electronic communications is the ECPA,[386] which includes three key components. The Wiretap Act regulates real-time interception of communications. It mandates a court order for wiretapping under stringent conditions, including proof that other investigative methods have failed.[387] The Stored Communications Act (SCA), which governs access to stored electronic data, allows law enforcement to obtain stored information

381. *See* U.S. Dep't. of Just., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, § ix-xii (2015) [hereinafter Searching and Seizing].

382. *See* U.S. CONST. amend. IV.

383. FED. R. CRIM. P. 41.

384. 28 U.S.C. § 1651.

385. *See* Meredith Mays Espino, *A Tale of Two Phones: A Discussion of Law Enforcement's Use of the All Writs Act to Enforce Apple to Open Private iPhones*, 43 RUTGERS COMPUT. & TECH. L. J., 97, 98-100 (2017); John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data under the All Writs Act,* 57 B. C. L. REV., 1403, 1403 (2016).

386. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. 99-508, 100 Stat. 1848.

387. *See* Searching and Seizing, *supra* note 381, at 168.

with a warrant under specific conditions.[388] The Pen Register/Trap and Trace Statute addresses the collection of non-content data, such as phone numbers, through devices that capture dialing or routing information.[389] While these legal frameworks were established well before technologies addressed in this Article have become accessible, they may still have at least partial applicability to such tools today.

1. Application Toward Real-time Communications

Pegasus's first set of features allows the operator to surveil live content as it is being communicated or created. Unlike traditional wiretapping technologies, Pegasus gains access to the device itself, enabling the operator to access the data being sent and received by the device. I suggest classifying the content accessible through these methods into three sub-categories. The first could be called live natural communications, or conversations. The second comprises live content which is not part of a natural communication between two living entities, like web searches, photos taken by users but not posted or shared with other people, notes, etc. The third includes live geolocation, which, I argue, can fit into one of the two previous categories, depending on the circumstances.[390]

When using the term "natural communication" in this Article, I refer to conversational communication, or the transfer of content between living entities. Indeed, section 2510 of the ECPA defines wire communication as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications."[391] Oral communications are defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[392] The definition of electronic communication is broader, encompassing "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photo-optical system."[393] Section 2516 allows law enforcement officers to petition for a warrant allowing the wiretapping of live content within these categories.[394] Under the literal meaning of these definitions, a Google search is certainly an electronic

388. 18 U.S.C. §§ 2701-2713.
389. 18 U.S.C. § 3127.
390. Pegg & Cutler, *supra* note 2.
391. 18 U.S.C. § 2510.
392. *Id.*
393. *Id.*
394. *See* 18 U.S.C. § 2516.

communication because the search includes a transfer of signals. But no living creature except for the user is typically part of that communication. Accordingly, I argue this is not a form of natural communication. The distinction, I argue, should be of legal significance.

a. Natural Communications

Natural communications, I argue, are apparently covered by the current Wiretap Statute. Messages transmitted via applications like WhatsApp or iMessage, whether oral, in writing, or through photos, are essentially analogous to content transmitted via SMS or regular phone calls (or by letters and postcards). Although encryption technologies and internet-based transmissions make messages transmitted via WhatsApp or iMessage inaccessible to law enforcement using older surveillance techniques, they do not receive additional legal protection. It seems unjustifiable to allow government surveillance of natural communications made through the regular phone application but restrict surveillance of identical conversations made through an application like WhatsApp. In other words, when spyware accesses live, natural communication, and that communication only, it could typically be perceived as equivalent to wiretapping. It should then accordingly be permissible under the Wiretap Statute of the ECPA.

The way the law defines the term "interception" could also support the claim that using Pegasus's ability to access live communications *is* wiretapping. Section 2510 states that "intercept means the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[395] This broad definition comfortably encompasses Pegasus's ability to access live communications.

b. Non-Natural Communications

The Wiretap Statute refers to *communications*. Can content from non-natural communications that are of a more technical nature, like a Google search, be viewed as a communication covered by a wiretap warrant? Though the language of the statute hints that this is indeed the case, I argue that the concept of natural communication should be taken into account, and that wiretap warrants should not allow the police to access non-natural communications.

Before the introduction of spyware of the sort of Pegasus, wiretapping was mostly irrelevant regarding non-natural communications. Traditional wiretapping technologies accessed natural communications, or conversations, by design: voice calls and text messages. Non-natural communications,

395. 18 U.S.C. § 2510.

like a photo taken but not shared, or a Google search, could not have been caught by these technologies, and would not have been perceived as "wiretapping" in the literal meaning of the term.[396]

The fact that these forms of content could be technically accessed by spyware that is also capable of wiretapping does not mean that a wiretapping warrant should allow access to these contents. Wiretapping has historically been understood as the act of intercepting or recording messages or voice conversations transmitted through natural communications, and has only recently become a more general term that describes other electronic surveillance activities.[397] But mixing the term wiretap with other forms of surveillance is misleading and, in this context, potentially harmful to the rights of suspects and defendants. Viewing suspects' browsing history or photo albums is not wiretapping, and a wiretap warrant seems accordingly unfit. Such a search, I argue, is much closer to a physical search of someone's belongings. It should accordingly be covered by a different legal framework, as will be discussed when addressing the second category of Pegasus's features, below. Despite the fact that the language of the Wiretap Statute may be perceived as covering non-conversational content, it does not seem to fit the original use and intent behind this mechanism.

c. Geolocation

Live geolocation information raises another set of considerations and questions. Currently, courts have not regarded phones as tracking devices, making warrants for the installation of a tracking device irrelevant in this context. The First Circuit explicitly found that a phone is not a tracking device under section 3117, citing *Carpenter*. The Court noted that warrants issued under section 3117 of the ECPA refer to the installation of a tracking device, which does not occur when a phone is being traced through CSLI.[398] This conclusion, however, seems far from obvious given current cyber technology, which *is* technically "installed" on a device.

When using CSLI to locate a phone, courts use the ECPA as the legal framework, specifically the SCA.[399] Nowadays, when communication technologies allow users to transmit their exact location not through CSLI but through internet-based and GPS technologies, can these

396. BRIAN HOCHMAN, THE LISTENERS: A HISTORY OF WIRETAPPING IN THE UNITED STATES, 23-24 (2022).

397. *See id.* at 23-24, 74.

398. United States v. Ackies, 918 F.3d 190, 199 (1st Cir. 2019).

399. *C.f.* Carpenter v. United States, 585 U.S. 296, 301-02 (2018).

messages be subject to wiretapping? To answer this question, a distinction should be drawn between whether the communication was an intended, natural communication, or a non-natural communication documented technically by the device, for instance for the user's own personal use.

Programs like WhatsApp allow users to send their location or a link that allows the recipient to track them for a limited timeframe. Apple allows iPhones to continuously broadcast their exact location to selected contacts. These are simply messages of a natural communicative quality, thus covered by the Wiretap Statute. However, Pegasus also allows the operator to access the live geolocation of an infected device, allowing access to geolocation information even if it was not communicated. Wiretaps, I argue, aim to surveil natural communications. Geolocation that was not shared with another individual is not a form of natural communication.

To summarize this point, the Wiretap Statute covers the government's ability to follow live communications between devices. It should not matter whether these communications use the cellular network or the internet, whether they are encrypted or not, and what exact technology allows the surveillance. However, other forms of live content accessed by Pegasus, such as live geolocation and live content that is not part of natural communication, do not seem to fit the traditional use of wiretap warrants. They should not be covered by a wiretap warrant, unless the legislator will specifically authorize such use.

2. Application Toward Stored Contents

Pegasus's second category of features grants the operator access to information stored on the device, including: past communications; content that is not part of a natural communication (e.g., photos, notes, or search history); and non-content information (e.g., previous numbers contacted or IP addresses).

Current legislation addressing electronically stored communications is outdated. The SCA is irrelevant in this context, primarily because warrants obtainable through it are aimed at a service provider. Section 2703 of the ECPA, dealing with the disclosure of customer communications, states, "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant."[400] Pegasus and similar programs do

400. 18 U.S.C. § 2703(a).

not request any service provider to disclose anything. Instead, they break into the phone and access the information directly. It seems far-fetched to use a framework that legally allows the government to require a third party to disclose information in situations where such a third party is not involved.

Moreover, due to the encryption mechanisms of these applications, the service provider generally could not access the information even if such an order was issued. For instance, WhatsApp encrypts messages end-to-end. Unlike cellular data providers, who can theoretically access information such as CSLI, WhatsApp or Apple cannot access the communications sent through their software.[401] If any law enforcement agency needs access to information transmitted through an encrypted service or saved on a device after encryption, requesting a section 2703 (d) order is futile because the provider cannot access the information. The agency must gain access to the device directly.

The Pen/Trap Statute is similarly unhelpful. It only grants access to limited data, such as dialing or routing information that is likely to identify the source of electronic communications.[402] However, orders issued under the statute apply to "any person or entity providing wire or electronic communication service."[403] If the electronic communication service cannot access the information, law enforcement agencies would not find these warrants helpful.

Given the ECPA offers no recourse, law enforcement agencies must rely on more generalized legislation to access stored, encrypted content on a phone using Pegasus. If searching a person's phone using spyware such as Pegasus is considered searching their cyberspace, and searching cyberspace is akin to searching a place, then a generalized search warrant under Rule 41 of the Federal Rules of Criminal Procedure makes sense. Though more helpful than the ECPA, Rule 41's framers likely did not envision tools like Pegasus. Rule 41 addresses electronic media by allowing the seizing and copying of information, including—when venue limitations arise—remotely, but does not address the constitutional questions that arise from the possibility of conducting such a search through concealed spyware, of the kind Pegasus allows.[404]

---

401. WhatsApp Help Center, *supra* note 105; Privacy, Apple, www.apple.com/privacy/ (Last visited Apr. 5, 2025) ("With groundbreaking privacy protections, it gives you peace of mind that no one else can access your data").

402. *See* 18 U.S.C. § 3127.

403. 18 U.S.C. § 3123.

404. FED. R. CRIM. P. 41(b)(6), (e)(2)(B), (f).

However, if we consider intruding on one's cyberspace legally similar to intruding their physical space, Rule 41 is a suitable framework for obtaining a warrant. In *Riley*, the Supreme Court noted that modern phones contain information once stored privately, like diaries and photo albums; the fact that people now carry this private information with them does not diminish its protection.[405] Therefore, media stored on a phone rather than in a drawer—I argue—should not be any less protected just because of the way it has been stored. To access a person's private diary, the police must obtain a warrant under Rule 41.

The ability to conduct these searches remotely using spyware does not change their nature: searches in a private space. Thus, a search warrant under Rule 41 is appropriate provided the limits set by the Rule.[406] A warrant allowing the police to target the photo album application on a phone does not permit searching any other application. Such a search is lawful under the current framework only if the spyware can access *only* the information authorized by the warrant. If the program grants broader access, it could violate the warrant and lead to unlawful searches. This applies regardless of whether the content is communicated to a third party (e.g., WhatsApp messages), is in the category of non-communicated content (e.g., private photos that were not shared), or is non-content (e.g., metadata).

Regarding stored location information, current doctrine suggests that a phone is not a tracker,[407] and a warrant to obtain CSLI through the ECPA would not suffice for this type of geolocation, as it is not stored on the service provider's servers. The correct method to obtain this information would be a search warrant pursuant to Rule 41. Geolocation history saved on a phone but not shared with a server is akin to a diary documenting one's movements, requiring a full search warrant.

This interpretation leading to Rule 41, however, may create an anomaly: obtaining information stored on a third-party service provider's servers could be harder than obtaining private information stored on a personal device, despite the latter being more intrusive. When warrant requests are made through the SCA or the Pen/Trap Statute, and even in cases where the All Writs Act is used, a third party can challenge the request. Service providers can refuse and challenge orders in court.[408] However, tools like Pegasus allow the government to obtain information

405. *See* Riley v. California, 573 U.S. 373, 393-94 (2014).

406. See FED. R. CRIM. P. 41(c)-(f).

407. *See* United States v. Ackies, 918 F.3d 190, 199 (1st Cir. 2019).

408. *See, e.g.*, *In re* Apple, Inc., 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

directly from the device without third-party assistance, often in secret, without the target's knowledge. Consequently, there is no one to challenge the warrant, making it, in certain aspects, easier to obtain a more intrusive warrant. This anomaly is concerning and should be addressed by the legislature.

It is also worth noting that Pegasus's capability of accessing stored content on a device allows operators to delete existing files from infected devices. There are two versions of this capability. The first involves deleting files created by Pegasus to hide the infection from the user.[409] As to the second, there is evidence that infected users noticed other files missing from their devices after infection.[410] A warrant pursuant to Rule 41 may be the proper vehicle for law enforcement to use spyware similar to Pegasus to obtain and remove information from a phone, storing it on law enforcement agency servers for later examination. Rule 41(e)(2)(B) authorizes the seizure or copying of electronically stored information, allowing examination and review "off-site."[411] Though initially framed for physical copying, the rule could apply to the remote copying and seizure of files. It does not seem to permit deleting files without copying them though. Therefore, no existing type of search warrant seems to authorize deleting files from a device without maintaining a copy, assuming Pegasus has been used for such purposes.

3. Application Toward Filming, Recording, and Tracing

The third and perhaps most intrusive category of capabilities offered by Pegasus and similar programs includes access to features that generate new content using the infected device. Pegasus can remotely activate the camera or microphone to initiate recording. Additionally, it can generate geolocation maps based on the device's location.[412] These functionalities do not constitute a search within the device or cyberspace; rather, they entail searching physical spaces, remotely.

Currently, law enforcement agencies may request warrants to access cameras or install different forms of hidden surveillance and bugging tools to intercept oral communications (including non-wire, non-electronic communication).[413] However, these devices are stationary and

409. O'Cearbhaill & Marczak, *supra* note 98, at 12.

410. *See id.*; Tidy, *supra* note 76. (discussing files missing from an infected device).

411. FED. R. CRIM. P. 41(e)(2)(B).

412. *See* RICHARD & RIGAUD, *supra* note 11, at 80-81 (mentioning the ability to view "geolocation history").

413. *See* 18 U.S.C. § 2518 (addressing the interception of wire, oral, or electronic communication). *See also* Lauren Cahill, *Ring Ring . . . No Answer, No Warrant, No Problem? A Look into a Hidden Cost of Home Surveillance Technology*, 61 SAN DIEGO L. REV. 683, 708 (2024).

do not follow the user, unless they are attached to a vehicle or a portable object. Thus, they are ill-suited to replicate the highly intrusive mechanism of using a phone as a dynamic hidden camera. The feasibility of employing such devices could be enhanced if programs like Pegasus incorporate a GPS-based feature to record automatically only when the phone is in a certain location. For instance, if law enforcement wishes to record the office of a senior official suspected of bribery, they can currently seek a warrant to install a camera in the relevant chambers. If Pegasus was used to automatically record only when the specific phone of the person in question is present, such a warrant could become applicable.

In some respects, this method may be less invasive than physically installing a camera in the chambers. It circumvents the need for physical installation of a bug and records only when the specific phone of the individual is in the room, rather than capturing continuous footage of the room in general. However, the widespread use of this feature to record and photograph a target without constraints or geographical limitations appears to fall outside the current legal framework, or at least not to be directly addressed by it, leaving significant room for interpretation.

Finally, the issue of tracking arises. U.S. courts have not considered phone tracking to fall under the Warrant for a Tracking Device provision of Rule 41,[414] and instead permitted law enforcement to obtain CSLI warrants using the SCA.[415] The main rationale provided is that while a Tracking Device Warrant requires "installation," accessing CSLI through a service provider does not necessitate any form of installation. However, tools like Pegasus differ significantly from accessing stored geolocation data through a service provider. Most notably, Pegasus's capabilities are more invasive due to their specificity and precision. Unlike CSLI technology, which relies on communication between a cell phone and the cellular network,[416] Pegasus accesses the GPS of the targeted device, achieving a higher degree of precision. Moreover, Pegasus requires installation, which challenges the notion that a phone does not qualify as a tracking device under Rule 41.

The distinction between tracking device warrants and SCA warrants seeking CSLI information is not merely theoretical. Tracking device warrants are more constrained, with Rule 41(b) limiting a district

414. *See* FED. R. CRIM. P. 41(e).

415. *See* United States v. Ackies, 918 F.3d 190, 194 (1st Cir. 2019).

416. *See* Alexander Porter, *Time Works Changes: Modernizing Fourth Amendment Law to Protect Cell Site Location Information*, 57 B. C. L. REV., 1781, 1781-82 (2016).

judge's jurisdiction to issue such warrants to persons or properties within the district (with exceptions).[417] The SCA does not impose such a strict restriction, and any "court of competent jurisdiction" could issue these warrants.[418]

In conclusion, existing legal frameworks do not adequately address the challenges posed by spyware such as Pegasus. While some interpretations suggest that certain features may be permissible, significant uncertainties remain. The Wiretap Statute seems to permit law enforcement agencies to intercept live phone communications, whether through spyware or traditional methods, as long as the interception involves communications. However, this statute does not extend to other forms of live content beyond communications. To distinguish between communications that should be accessible under the Wiretap Statute and non-natural communicative content that should remain inaccessible, I argue it is beneficial to apply a "natural communication test." This test would help differentiate the type of natural communication that clearly falls under wiretap provisions from technical communications that I think should not be included.

Accessing stored content is outside the scope of the Stored Communications Act (SCA), which requires service providers to disclose information rather than directly intruding into a phone. This finding supports the argument made in Section V.A.2, where it was asserted that penetrating a phone and examining its stored contents is analogous to searching a physical space. As a result, some stored information may be accessible through standard Rule 41 search warrants. This also applies to the remote seizure of files and content, which could be covered by Rule 41.

Finally, the ability to generate new content, such as recording or tracking a device, does not constitute a search of the *phone*. Instead, it effectively transforms the device into a highly invasive tracking device or concealed camera in a physical space. While some aspects of this feature may fall under existing Rule 41 principles, ambiguity in these legal doctrines, particularly in light of the previous circuit court ruling that questioned whether phones qualify as tracking devices under Rule 41 and the SCA, creates a murky legal landscape.

This uncertainty is far from ideal, as the law has yet to directly address advancements in commercial spyware use. As a result, this situation

417. FED. R. CRIM. P. 41(b).

418. Stephen Wm. Smith, *Why are Precise Location Warrants a Thing?*, CTR. FOR INTERNET AND SOC'Y AT STAN. L. SCH. (Dec. 10, 2019), www.cyberlaw.stanford.edu/blog/2019/12/why-are-precise-location-warrants-thing/.

could lead to confusion and, ultimately, contentious debates over the legality of practice and admissibility of evidence. The subsequent section of the Article explores how other nations are navigating this new era of cybersurveillance, drawing lessons from their experiences, as presented in Section III.C. The Article then proposes strategies within the existing legal framework and offers policy considerations for lawmakers and judges to consider in the future.

B. *Facing the Pegasus Era*

The existing legal framework appears to allow law enforcement agencies to use some features offered by Pegasus and equivalent products. Other features seem to fall outside the purview of any existing legislation. Furthermore, the mechanisms that are theoretically covered by existing legislation are subject to different statutes. A wiretap warrant does not cover a search of stored content, and a search warrant does not cover wiretapping. In other words, current U.S. legal doctrine reveals some gaps when trying to suggest Pegasus and similar solutions is operable under current legal frameworks. In some contexts, these gaps could be filled, either awkwardly or not, by current legislation. In others, new legal frameworks are required. This section first offers initial steps, including several policy recommendations that could be considered even without legislation or serious legal reforms. It then suggests broader legal reform may also be required in the foreseeable future and offers initial paths toward new legislative and legal doctrines on a higher level.

1. Policy Recommendations under Existing Legal Doctrine

First, it is crucial to ensure that law enforcement agencies can only access capabilities currently covered by law. This means that they should only be able to obtain "modular" versions of spyware that allow them to access only the information they are permitted to acquire. For example, since a wiretap warrant only allows the police to monitor live communications, and if a search begins at the time of infection, the police, covered by a wiretap warrant but without any other search warrant, should only be allowed to infect the target with a version of the program that allows limited access to live natural communications and live natural communications alone. Infecting a device with another version of the program should be considered an unwarranted search.

As discussed in Section III.C, the Merari Report of Israel and the EU Parliamentary report revealed that NSO was willing to sell modular versions of their program. In Germany, despite initial rejection of the

governmental request to limit the program, NSO eventually sold a modular version.[419] In Israel, the program was limited and did not present every feature Pegasus could offer, though the Ministry of Justice recommended further limitations.[420] A first step would be to ensure that when negotiating with these companies before buying their products, law enforcement agencies must only acquire modular versions of the program that allow them to infect a device in a way that will permit them to conduct searches only in limited types of content. That is, if a wiretap warrant is issued, only live natural communications are accessed by the program.

Second, law enforcement agencies should ensure that judges are fully aware of what they are authorizing when they issue a warrant. In the Israeli example, for instance, it was not clear that judges were fully aware they were approving the use of Pegasus, rather than traditional wiretapping.[421] In the United States, using existing legal frameworks to allow surveillance with these modern tools could raise a similar concern of misleading judges. It is crucial for judges to understand what they are authorizing when they sign a warrant.

Accordingly, it is recommended that the forms used to request search and wiretap warrants using spyware be updated to reflect the availability of these tools. Noting that the police must report back to a judge after conducting the search, for example, by returning the warrant,[422] it is evident that the legislature has expected judges to closely regulate the exact way the searches they approve of are being performed. It is accordingly recommended to adopt the relevant procedures and practices to ensure judges understand what type of technology is being used to execute the warrants they issue, and that the orders themselves precisely reflect what they allow and what they do not allow, even if they use existing legal frameworks.

Third, as previously discussed, the legislature should be required to review the Wiretap Statute to determine whether non-natural electronic communications—such as a photo taken and stored but not shared, or a Google query—should fall within the scope of wiretap warrants. Considering the likely intent of the legislature and the traditional use of wiretap warrants to intercept messages and conversations rather

419. PEGA report, *supra* note 108, ¶ 365 (discussing how the German Federal Criminal Police Office asked NSO to "write a source code, so that Pegasus would only be able to access what was allowed by the law".).

420. MERARI ET AL., *supra* note 40, at 42.

421. *See id.* at 46-47.

422. FED. R. CRIM. P. 41 (e) (2) (A) (iii).

than technical communications or non-content data, and the difference between the term "wiretap" and the term "electronic surveillance,"[423] I argue that wiretap warrants are not the appropriate framework for accessing non-natural communications or electronic interactions between a human and a machine. In this context, the legislature might look to the Israeli wiretap warrant as a model. In Israel, a wiretap warrant applies only to the interception of a "conversation" between "participants in a conversation."[424] A similar definition would allow wiretap warrants to target natural communications or conversations while addressing technical communications through more appropriate legal frameworks, such as the Stored Communications Act (SCA).

Fourth, knowingly accessing a computer without authorization is a crime.[425] The ECPA states that those who illegally intercept wire, oral, or electronic communications shall be punished.[426] Accordingly, it is worth bearing in mind that ex-post exclusion of evidence that was illegally obtained by spyware might not be sufficient to combat the potentially abusive usage of these programs in practice. In certain cases, using these tools could be a criminal offense and put the relevant officers in danger of prosecution.

2. Amending Statutes and Rethinking Legal Doctrine

The Electronic Communications Privacy Act (ECPA) was enacted in response to the unique nature of electronic media. But it was designed for a different technological era. While existing legal frameworks can still be leveraged to obtain warrants for certain cyber searches, these frameworks require significant interpretational efforts. Ideally, this new era of cybersurveillance should prompt a reassessment of the scope of access available to law enforcement agencies. I propose several initial considerations for this reevaluation process.

First, in Section V.A.1, I argued that law enforcement agencies can currently obtain access to stored content through Rule 41 search warrants. This legal structure treats cyber searches analogously to physical searches, which could be advantageous if we take the metaphor of cyberspace as a place seriously. However, unlike physical searches, where the target can often discover that their premises have been searched, advanced cybersurveillance technologies may leave the target unaware of the search.

423. *See* HOCHMAN, *supra* note 396, at 23-24.

424. Secret Monitoring Law, 5739–1979, SH 50 141, art. 1 (Isr.).

425. *See* 18 U.S.C. § 1030.

426. 18 U.S.C. § 2511.

As discussed in Section V.A.2, current legal frameworks for searching stored electronic data impose rigorous mechanisms for obtaining a warrant. For example, the SCA enables warrants to be issued that allow access to content through the service provider. The service provider can challenge the warrant if it believes it has been improperly issued. Major tech companies, including Google, Meta, and Apple, have reported that they do not comply with every order issued to them.[427] However, spyware programs, by their technical nature, do not require the cooperation of third parties. This creates somewhat of an anomaly: Rule 41 search warrants permit more intrusive and easily executed searches, which typically cannot be challenged, while SCA warrants can be contested.

One potential solution is to require law enforcement agencies to inform third parties—such as service providers—of the warrant, giving them an opportunity to contest it even if their cooperation is not technically necessary for the search. Another option is to establish an internal review mechanism within the U.S. Department of Justice to assess these warrants before execution, or to mandate that a senior prosecutor or investigator from another agency approve each order request before it is submitted.

Second, the availability of these tools may necessitate a reconsideration of the list of crimes that justify requesting such a warrant. The Wiretap Statute currently contains a comprehensive list of offenses that could warrant wiretapping.[428] Because a warrant that enables a search with spyware such as Pegasus would be more intrusive than ordinary wiretapping, it makes sense to reevaluate this list and to legislate that Rule 41 search warrants targeting devices with Pegasus be subject to a similar, or perhaps even more restrictive, list of offenses. The examples set by Israel and Germany can offer guidance for such a list. However, in both cases, the lists are quite comprehensive and could perhaps be reduced to a shorter list of exceptionally severe criminal activities, such as homicide, drug trafficking, or human trafficking.

Third, the availability of spyware such as Pegasus necessitates rethinking the legal definition of tracking devices. As mentioned, current legal frameworks do not typically classify phones as potential tracking devices. One reason for this is that no physical device is "installed" when a phone is tracked using cell-site location information (CSLI). These

427. *See, e.g.*, *In re* Apple, Inc., 149 F. Supp. 3d 341 (E.D.N.Y. 2016). *See generally Transparency Reports*, META, www.transparency.meta.com/reports/ (last visited: Feb 18, 2025); *Transparency Reports*, GOOGLE.COM, www.transparencyreport.google.com/ (last visited: Feb 18, 2025); *Transparency Reports*, APPLE.COM, www.apple.com/legal/transparency/ (last visited: Feb 18, 2025).

428. *See* 18 U.S.C. § 2516.

new technologies change this dynamic, as spyware is indeed "installed" on a device to track it. It is therefore reasonable to define in legislation when exactly a phone is considered a tracking device and what kind of information can be accessed using a Rule 41 tracking warrant.

It is also important to recognize that location information is shared today in various ways. It can be part of natural communications or a mere record maintained by the device or service provider (though still, technically, a form of communication). Thus, it should be determined whether location information naturally communicated is covered by a wiretap warrant; whether there is a distinction between short-term natural communication of location (such as that offered by WhatsApp) and permanent communication (such as that provided by Apple on iPhones); and whether there is a difference between installing a physical tracking device and installing spyware on a phone, which effectively turns it into a tracking device.

VI. Conclusion

We have entered the Pegasus Era, a new age of cybersurveillance in which every phone can potentially become a spy in one's pocket. Governments have been employing these technologies for years. To date, scholarship and media coverage have primarily focused on the abuse of these products by authoritarian regimes. However, liberal democracies have also gained access to these technologies for the purpose of law enforcement. It is likely that law enforcement practices will increasingly rely on them in the coming years.

This Article presented three main arguments. First, it highlighted how technological advancements, particularly the widespread use of encrypted communications, are rendering traditional surveillance methods less effective, leaving law enforcement "in the dark." In response, I argued that spyware should not be viewed as a monolithic solution but rather as a diverse toolbox, with each tool's features warranting distinct levels of legitimacy and regulation depending on their use in law enforcement practices. Based on the comparative experience, this Article argued that it is crucial to define how exactly these tools could be used.

Second, this Article examined the intersection of commercial spyware and the Fourth Amendment. It argued that using these tools to access content on a private device constitutes a search under the Fourth Amendment and could be interpreted as a form of trespass. Furthermore, it contended that the search begins at the moment of infection, not merely when the content is accessed, and hence a warrant must be obtained before the device is infected.

Third, the Article proposed classifying the known features of spyware into three categories: the ability to surveil live content, access and remove stored content, and create new content using the device's hardware. It then analyzed how current U.S. legal frameworks align with these capabilities. I argued that some features, such as the ability to wiretap real-time encrypted communications, are covered by existing legislation, while others are not. I further suggested that the capabilities not currently addressed by existing legal frameworks should be the focus of new legislative and jurisprudential efforts. I provided key policy recommendations for how these gaps could be filled.

The Pegasus Era is not approaching; it is already here. As technology advances, crime becomes more sophisticated as well. It is therefore crucial for law enforcement agencies to develop new, up-to-date methods to face this evolving landscape. However, reality has proven that when the government employs new technological abilities to face modern crime, these can be easily abused. It is time for U.S. policymakers to directly address this new age of cybersurveillance and ensure that the U.S. criminal justice system is well-equipped to face it. As we move deeper into the Pegasus Era, it is crucial that our legal and ethical frameworks evolve in tandem with technological advancements. Only through proactive regulation can we hope to harness the potential of these powerful surveillance tools while safeguarding the fundamental principles of privacy and due process that underpin democratic society.