Harvard Journal of Law & Technology
Volume 34, Number 2 Spring 2021

STINGRAY STUNG? ANALYZING CELLPHONES AS EFFECTS PROVIDES FOURTH AMENDMENT TREATMENT

*Roya Butler**

TABLE OF CONTENTS

I. INTRODUCTION

The Fourth Amendment protects the rights of the "people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1] It further provides that "no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."[2] This judicial safeguard was designed to protect against the government's use of general warrants to conduct broad and indiscriminate searches with impunity.[3] In this way, the Framers "sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations."[4] The

* Georgetown Law, J.D., 2020. Much appreciation to Dean Paul Ohm whose encouragement to write about Stingrays and supervision of my research led to this Note. Many thanks to Professor Michael Dreeben for his insights on Fourth Amendment jurisprudence and for his continued mentorship and friendship. My gratitude to Professor Laura K. Donohue for taking the time to make valuable suggestions during final editing. Thank you to Jordan Kennedy for his feedback, care, and support; and to Rachel Pester and the other editors of the Harvard Journal of Law & Technology for their meticulous edits and thoughtful comments that assisted me in refining my Note.

1. U.S. CONST. amend. IV.

2. *Id.*

3. *See* Scott D. Blake, *Let's Be Reasonable: Fourth Amendment Principles in the Digital Age*, 5 SEVENTH CIR. REV. 491, 521 (2010).

4. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

Framers restricted the government's power to search and seize to prevent the government from accessing information in a person's home, papers, and effects that provide undue insight into a citizen's beliefs.[5]

A magistrate may issue a warrant if the government can show probable cause for its allegations.[6] The warrant must "particularly describe the things to be seized" so that "nothing is left to the discretion of the officer executing the warrant."[7] This particularity requirement ensures that the search will be narrowly tailored and "will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[8] The Supreme Court has held that reasonableness is the touchstone of any Fourth Amendment analysis.[9] A search's reasonableness "is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[10]

Stingrays, manufactured by Harris Corporation, have become the generic name for cell-site simulators ("CSS"), and are also referred to as international mobile subscriber identity-catchers ("IMSI-catchers").[11] These devices can passively collect cellular transmissions and decode the signal to locate and track the IMSI, or actively exploit cellphones to connect and transmit GPS and other sensitive data.[12]

---

5. Laura K. Donahue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing a Test Consistent with Precedent and Original Meaning*, 2018 SUP. CT. REV. 347, 348.

6. Blake, *supra* note 3 (citing United States v. Ross, 456 U.S. 798, 824 (1982)).

7. Marron v. United States, 275 U.S. 192, 196 (1927); *see also* Stanford v. Texas, 379 U.S. 476, 485 (1965).

8. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

9. Illinois v. McArthur, 531 U.S. 326, 330 (2001); Katz v. United States, 389 U.S. 347, 359 (1967).

10. Delaware v. Prouse, 440 U.S. 648, 654 (1979).

11. *Cell-Site Simulators/IMSI Catchers*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers [https://perma.cc/LR88-ZA5P]. Although all are generally referred to colloquially as "Stingrays," cell-site simulators are also manufactured by Atos, Rayzone, Martone Radio Technology, Septier Communication, PKI Electronic Intelligence, Datong (Seven Technologies Group), Ability Computers and Software Industries, Gamma Group, Rohde & Schwarz, Meganet Corporation. *Id.*; *see also* Jason Koebler, *This App Claims to Know when Police Are Tracking You with Fake Cell Towers*, MOTHERBOARD (Dec. 30, 2014, 1:50 PM), https://web.archive.org/web/20160304135818/http://motherboard.vice.com/read/this-app-claims-to-know-when-police-are-using-fake-cell-towers-to-track-you [https://perma.cc/D6MT-XAH2]; Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, INTERCEPT (Sept. 12, 2016, 2:33 PM), https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/ [https://perma.cc/3BGL-XWW7].

12. *Cell-Site Simulators/IMSI Catchers*, *supra* note 11. Stingrays can collect information including unique identifiers, such as IMSI (International Mobil Subscriber Identity) and ESN (Electronic Serial Number); meta data (time on calls made and numbers dialed); text messages; and websites visited.

Stingrays can be handheld by an officer or mounted in vehicles, airplanes, helicopters, or drones.[13] Law enforcement officers use Stingrays to locate the mobile devices of target suspects.[14] They can then gather the global positioning system ("GPS") information to identify suspects, or locate them through triangulation.[15] Stingrays masquerade as genuine cell towers,[16] tricking mobile devices in their vicinity into transmitting information including location data, text, and voice communications to them.[17] Stingrays collect this data indiscriminately, not only from the suspect but from all cellphones in the area.[18]

Stingrays were originally designed for military warfare, to infiltrate enemies' communications systems,[19] and are currently owned by sev-

---

13. Curtis Waltman, *Here's How Much a StingRay Cellphone Surveillance Tool Costs*, VICE (Dec. 8, 2016, 11:00 AM), https://www.vice.com/en_us/article/gv5k3x/heres-how-much-a-stingray-cell-phone-surveillance-tool-costs [https://perma.cc/3EZ2-RKBZ].

14. Kim Zetter, *How Cops Can Secretly Track Your Phone*, INTERCEPT (July 31, 2020, 7:00 AM), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [https://perma.cc/KA37-76R2]; *see also* Biddle, *supra* note 11; Jeremy Scahill & Margot Williams, *A Secret Catalogue of Government Gear for Spying on your Cellphone*, INTERCEPT (Dec. 17, 2015, 12:23 PM), https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/ [https://perma.cc/AB8B-L7AU].

15. *See In re* Application of United States for an Ord. Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 534 (D. Md. 2011) (explaining that "[w]hile GPS location technology locates a user by triangulating satellite signals, 'cellular identification locates a user by triangulating their position based on the cell towers within signal range of their mobile phone'"). By gathering cellphone signals in proximity to the suspect and from other locations where he is present at other times, law enforcement can use triangulation to locate the suspect. Lisa M. Schaffer, *Police Use of Surveillance Stingrays Requires a Warrant*, FINDLAW (Sept. 19, 2018, 6:57 AM), https://blogs.findlaw.com/blotter/2018/09/police-use-of-surveillance-stingrays-requires-warrant.html [https://perma.cc/54KK-KU2T] (noting that the police used a Stingray to triangulate the suspect's position); Nicole Valdes Hardin, *Cell Phone Surveillance: Tactics, Litigation, and Next Steps*, OFF. OF THE FED. PUBLIC DEF. — E. DIST. OF VA. (Apr. 2018), https://vae.fd.org/sites/vae.fd.org/files/training/April_2018/03%20Cell%20Phone%20Surveillance.pdf [https://perma.cc/3AS8-BWHN] (explaining how cellphone triangulation works).

16. *Cell-Site Simulators/IMSI Catchers, supra* note 11.

17. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013) (finding the respondents' claim that their communications were likely being monitored as "too speculative"). By emitting a strong signal, Stingrays mimic a cellphone tower. This causes all cellphones in the surrounding area to connect to the Stingray, amassing location data, text, and voice communications. *Id.*

18. Adam Bates, *Stingray: A New Frontier in Police Surveillance*, CATO (Jan. 25, 2017), https://www.cato.org/publications/policy-analysis/stingray-new-frontier-police-surveillance [https://perma.cc/WE2X-H76Y] (quoting U.S. DEP'T OF JUST., ELECTRONIC SURVEILLANCE MANUAL 40–41 (June 2005)).

19. John Haystead, *Optical Warfare: Technology Emerges to See the Enemy, and to Blind Him*, MIL. & AEROSPACE ELECS. (Mar. 1, 1997), https://www.militaryaerospace.com/communications/article/16710290/optical-warfare-technology-emerges-to-see-the-enemy-and-to-blind-him [https://perma.cc/7VYY-5BE6]. Stingrays were originally developed for the U.S. Army. Attached to fighting vehicles, Stingrays were created with the purpose of

enty-five agencies in twenty-seven states and the District of Columbia.[20] Stingray's can employ Man-in-the-Middle ("MITM") attacks to listen to or record calls, send messages as if they are coming from the target phone, download contacts and photos, or inject malware into targeted phones.[21] Since 2006, the government has employed Stingrays in the course of many criminal investigations.[22] Federal agencies, including the Federal Bureau of Investigation ("FBI"), the Drug Enforcement Administration ("DEA"), the National Security Administration ("NSA"), the Department of Homeland Security ("DHS"), and the U.S. Immigration and Customs Enforcement ("ICE") are known to be using these devices.[23]

In one case, a woman alerted law enforcement that she was assaulted and that her purse and phone had been stolen.[24] Less than twenty-four hours later, without a warrant, the Tallahassee, Florida police obtained real-time cellphone location information ("CSLI")[25] from her service provider.[26] The CSLI provided the officers with a radius in which to search for the perpetrator and the cellphone's IMSI, which allowed the police to accurately track the phone.[27] Law enforcement used the hand-held Stingray to locate the suspect within an apartment complex, and "determine[d], with relative certainty . . . the particular area of the apartment that the [cellphone] was emanating from."[28] The Stingray seized data not only from the targeted IMSI, however, but also from every cellphone in the radius, including specific location coordinates from inside people's homes.[29]

---

detecting, tracking, and neutralizing fire-control systems "on enemy ground vehicles and aircraft beyond their effective fighting range." *Id.*

20. *Stingray Tracking Devices: Who's Got Them?*, ACLU (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [https://perma.cc/K6RU-4WGW] [hereinafter *Stingray Tracking Devices*].

21. Matthew Hughes, *What is a Man-in-the-Middle Attack?*, HOW-TO GEEK (May 13, 2020, 6:40 AM), https://www.howtogeek.com/668989/what-is-a-man-in-the-middle-attack/ [https://perma.cc/J9Y2-S87V] (explaining that an MITM attack occurs when a device sits in the middle of two devices, intercepting communication traffic).

22. *See* Bates, *supra* note 18.

23. *Id.* Stingrays are also used by the Marshals Service, the Secret Service, and the Department of Homeland Security. Zetter, *supra* note 14.

24. Cyrus Farivar, *How Florida Cops Went Door to Door with Fake Cell Device to Find One Man*, ARS TECHNICA (June 4, 2014, 12:38 PM), https://arstechnica.com/tech-policy/2014/06/how-florida-cops-went-door-to-door-with-fake-cell-device-to-find-one-man/ [https://perma.cc/4QQ2-NTTP].

25. *Id.* CSLI refers to information collected as a cellphone identifies its location to nearby cell towers.

26. *Id.*

27. *Id.*; *see also Computer Security Resource Center*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/IMSI [https://perma.cc/6EAL-BAJ3].

28. *Id.* A hand-held Stingray is also known as a Kingfish. Zetter, *supra* note 14.

29. Zetter, *supra* note 14.

Is the search reasonable under the Fourth Amendment if the Stingray indiscriminately sweeps all cellphone data in its radius? The Founders rejected general warrants, which allowed the government to search without limitation or specific description of the object of the search.[30] To protect against authorizations of such far reaching searches, warrants required particularity to be valid under the Fourth Amendment. [31] Stingrays conduct broad and indiscriminate searches with free reign, rather than specific searches of a targeted device, and in this way function more like a general warrant.[32] Although a phone thief may have no reasonable expectation of privacy in the stolen phone,[33] this same surveillance intrudes upon even lawfully owned phones in the area with impunity. Establishing probable cause to allow a Stingray to interfere with surrounding phones in the area would be a difficult proposition. The warrant could not presumably describe with particularity the phones in the targeted area because Stingray operations are conducted in real-time.

Although some agencies claim to use Stingrays only for IMSI acquisition, there is evidence that they can intercept data, "divert calls and text messages, edit messages, and even spoof the identity of a caller in text messages and calls." [34] For example, the Department of Justice's Electronic Surveillance Manual leaves open the possibility of mass data collection so that law enforcement agents using Stingrays could collect "the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's [electronic serial number], the date, time, and duration of the call, and the cell-site number/sector (location of the cellular telephone when the call was

30. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1192 (2016) (illustrating the historical overriding concern for general warrants). The revolution largely was based on the opposition to the Crown's effort to exercise writs of assistance, which allowed generalized searches by the Crown. Several states ratified the U.S. Constitution under the condition that the document would be amended to prohibit indiscriminate searches and seizures. *Id.* at 1194.

31. *Id.* at 1192.

32. Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance,* ACLU (Nov. 17, 2017, 1:45 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/what-founders-would-say-about-cellphone-surveillance [https://perma.cc/ZN6G-H3L6] (discussing general warrants and noting that general searches are per se unreasonable); David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425, 458 ("General warrants are unreasonable."); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 601 (1999) ("The historical record . . . reveals that the Framers focused their concerns and complaints rather precisely on searches of houses under general warrants [when drafting the Fourth Amendment].").

33. *See* Rakas v. Illinois, 439 U.S 128, 143 n.12 (1978) (noting that a "burglar plying his trade" does not have an expectation of privacy "which the law recognizes as 'legitimate'").

34. *Cell-Site Simulators/IMSI Catchers*, *supra* note 11 (citing *3G-GSM Tactical Interception & Target Location*, GAMMA GROUP, https://info.publicintelligence.net/Gamma-GSM.pdf [https://perma.cc/VQ95-8L4J]); *see also* Bates, *supra* note 18 (quoting U.S. DEP'T OF JUST., ELECTRONIC SURVEILLANCE MANUAL 40–41 (June 2005)).

connected)," and the contents of the communication.[35] Some courts, noting the element of involuntariness, have ruled that the use of CSS requires a warrant.[36] Although the Department of Justice's internal policy prohibits the use of CSS to collect information other than GPS data, this policy does not bind state and local governments.[37] Nevertheless, states are trending towards legislation banning the use of CSS without a warrant.[38] For example, New York has proposed legislation to ban warrantless electronic data collection; California, Utah, Virginia, and Washington have passed similar legislation.[39]

This Note discusses the use of Stingrays and examines the original meaning of effects under the Fourth Amendment and its application to their use. Part II provides a brief description and explanation of Stingray CSS technology and operation. Part III analyzes the development of Fourth Amendment jurisprudence, including the Supreme Court's recent decision in *Carpenter*. In Part IV, this Note examines the Fourth

---

35. U.S. DEP'T OF JUST., ELECTRONIC SURVEILLANCE MANUAL 40–41 (June 2005). The cellphone number, the 10-digit unique number that a wireless carrier uses to identify a mobile phone, is known as MIN. The international mobile subscriber identity (IMSI) contains the MIN. The ESN was introduced by the Federal Communication Commission in the early 1980s as a unique identifier as a tool to track phones or ban them from a network. Jason Fitzpatrick, *What is an ESN, and Why Do I Care if it's Clean?,* HOW-TO GEEK (Nov. 3, 2016, 5:22 PM), https://www.howtogeek.com/172849/ask-htg-whats-an-esn-and-why-do-i-care-if-its-clean/ [https://perma.cc/AP44-9J9W]; Marshall Brain et al., *How Cell Phones Work,* HOWSTUFFWORKS, https://electronics.howstuffworks.com/cell-phone3.htm [https://perma.cc/6A8Q-FZF8] (defining MIN and ESN); *see also In re* Application of the United States for an Ord. Relating to Tels. Used by Suppressed, No. 15-0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015) (noting that Stingrays capture "a vast array of information, including, but not limited to, the cell phones' electronic serial number (ESN) or international mobile subscriber identification (IMSI)").

36. *See, e.g.*, United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (finding that "[a]bsent a search warrant, the government may not turn a citizen's cellphone into a tracking device"); Jones v. United States, 168 A.3d 703, 707 (D.C. 2017) (holding that the government violated the Fourth Amendment when it deployed the cell-site simulator without first obtaining a warrant based on probable cause); *see also* State v. Andrews, 227 Md. App. 350, 393 (Md. Ct. Spec. App. 2016) (requiring a search warrant to use a CSS); State v. Tate, 357 Wis. 2d 172, 189 (Wis. 2014) (assuming, without deciding, that use of a Stingray amounted to a Fourth Amendment search requiring a warrant).

37. *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, U.S. DEP'T OF JUST. (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [https://perma.cc/PDA9-3Z8R] (restricting CSS use to gathering GPS and only with a warrant).

38. Kevin Collier, *How Police Use 'Stingray' Devices to Secretly Track Your Phone*, WEEK (Apr. 26, 2017), https://theweek.com/articles/694360/how-police-use-stingray-devices-secretly-track-phone [https://perma.cc/T3B3-5237]. California, Utah, Virginia, and Washington require a warrant for their use, and to date there is no federal law that regulates them. *Id.*

39. *Id.* New York Assembly Bill 2620 (A2620) and companion bill (S4619), introduced in January 2019 and carrying over to the 2020 legislation aim to ban the use of Stingrays to track cellphone location as well as mass electronic data collection. Assemb. 2620, 2020–21 Assemb., Reg. Sess. (N.Y. 2021). CAL. PENAL CODE § 1546.1 (West 2015); WASH. REV. CODE § 9.73.260 (2015); VA. CODE ANN. § 19.2-70.3 (2015); UTAH CODE ANN. § 77-23c-102 (West 2014).

Amendment analysis for Stingray interference with cellphone signals and how that compares to precedent involving modern technology. Finally, Part V demonstrates that the original meaning of Fourth Amendment effects protects cellphones.

II. STINGRAY OPERATION AND TECHNOLOGY

By default, phones connect to the strongest signal tower.[40] A Stingray exploits this function with a MITM attack using its strong signal transmission as a means to surreptitiously force temporary connections with in-range cellular devices, exchanging data as the phone would with a cellphone tower.[41] Once the phone connects to the Stingray, the operator can locate the phone's physical location.[42] The international mobile subscriber identity ("IMSI") reveals the user's country code, user account, network code, and telephone number, and allows the phone to communicate with the cellular network.[43] Once the Stingray obtains the IMSI of the cellphone, "it releases the cellphone so that it can connect to a legitimate cell tower, allowing data and voice calls to go through."[44] This "catch-and-release" downgrade attack employed

40. *See* Summer Hirst, *How to Avoid Stingray Downgrade Attacks*, Private Internet Access (Dec. 7, 2018), https://www.privateinternetaccess.com/blog/2018/12/how-to-avoid-stingray-downgrade-attacks/ [https://perma.cc/7G22-4Y62]. The common protocol of cellular communication is to connect to the cell-site offering the strongest signal. *See also* United States v. Temple, No. S1415CR2301JARJMB, 2017 WL 7798109, at *27 (E.D. Mo. Oct. 6, 2017), *report and recommendation adopted*, No. 4:15-CR-230-JAR-L, 2018 WL 1116007 (E.D. Mo. Feb. 27, 2018) (citing Howard W. Cox, *Stingray Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FEDERALIST SOC'Y REV. 29, 29–30 (2016) (noting that cellphones by design connect to the closest cell tower with the strongest signal)).

41. Hughes, *supra* note 21; *see also* Cyrus Farivar, *Judge Slams FBI for Improper Cellphone Search, Stingray Use*, ARS TECHNICA (July 18, 2018, 6:00 AM), https://arstechnica.com/tech-policy/2018/07/judge-slams-fbi-for-improper-cellphone-search-stingray-use/ [https://perma.cc/7TFR-DXEC].

42. United States v. Patrick, 842 F.3d 540, 542–43 (7th Cir. 2016) (quoting U.S. DEP'T OF JUST., USE OF CELL SITE SIMULATOR TECHNOLOGY 2 (2015)).

43. A. Ghayas, *What is the Difference Between IMEI and IMSI Numbers?*, COMMSBRIEF (Sept. 20, 2019), https://commsbrief.com/what-is-the-difference-between-imei-and-imsi/ [https://perma.cc/7XPF-TSHN]. IMEI number is unique to the mobile device, and it can be used to protect the phone from being misused if stolen. In case a mobile phone is lost or stolen, the customer should immediately contact their mobile service provider. If the phone is lost (and not stolen), the mobile service provider might only block the SIM, but if the phone is stolen, they can use the IMEI number to block the phone, which will "blacklist" the phone from being used on any network. IMSI stands for International Mobile Subscriber Identity, and it is a unique number assigned to the SIM card used by the mobile subscriber. IMSI is usually a 15-digit number that identifies the mobile user within the mobile network. In order to ensure confidentiality of the mobile user, the network uses a temporary number known as TMSI (Temporary Mobile Subscriber Identity) during most of the communication with the mobile phone. *Id.*

44. *Id.*

by Stingrays causes interference with the cellphone's signal, which disrupts the phone's calling and texting functions.[45]

Downgrade attacks use network vulnerabilities to force a security downgrade.[46] More specifically, a downgrade attack uses a vulnerability that causes phones to switch from a high-quality mode of operation (e.g., 5G) to a lower quality and less secure mode of operation (e.g., 2G), typically provided by the cellular providers for older phone models.[47] By jamming more secure 5G, 4G LTE, or 3G network channels, Stingrays force cellphones to switch to a less secure, unencrypted 2G channel.[48] In other words, these attacks lower security measures to an older and less secure communications protocol.[49] To be sure, 5G was developed with more comprehensive encryption to protect against these fake base station attacks, but, inevitably, the security protections fell short because cellphones register unencrypted identifying information when connecting to cell towers.[50] Attackers can use this information to identify and locate the targeted device. To protect against this attack, carriers must build their systems to launch security protections and encryption upon connection.[51] Only nine out of thirty carriers in Europe,

---

45. Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015, 4:55 PM), https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/ [https://perma.cc/9DG9-ZCLQ].

46. Hirst, *supra* note 40.

47. Lily Hay Newman, *5G Is Here — and Still Vulnerable to Stingray Surveillance*, WIRED (Aug. 3, 2019, 7:00 AM), https://www.wired.com/story/5g-security-stingray-surveillance [https://perma.cc/M8S3-N6W4] [hereinafter *5G Is Here*]; *see also* Lily Hay Newman, *Holes in 4G and 5G Networks Could Let Hackers Track Your Location*, WIRED (Feb. 26, 2019, 2:56 PM), https://www.wired.com/story/torpedo-4g-5g-network-attack-stingray [https://perma.cc/V9VK-2NHB].

48. *See* Newman, *5G Is Here*, *supra* note 47 (explaining that "higher-category devices look for the 5G or 4G network, but low-category devices only accept 2G or 3G connections, because they don't need faster speeds. The researchers found that they could use their first stingray attack to . . . downgrad[e] it to an older network."); *see also* Altaf Shaik & Ravishankar Borgaonkar, *New Vulnerabilities in 5G Networks*, CONFERENCECAST (Aug. 7, 2019), https://www.conferencecast.tv/talk-20263-new-vulnerabilities-in-5g-networks#.talkPage-header [https://perma.cc/2FQV-XDEU].

49. *See Downgrade Attack*, PCMAG, https://www.pcmag.com/encyclopedia/term/downgrade-attack [https://perma.cc/6NKC-QM6R] (discussing vulnerabilities in devices that are built to support lower quality protocols); *see also* Zack Whittaker, *Security Flaw Shows 3G, 4G LTE Networks are Just as Prone to Stingray Phone Tracking*, ZDNet (July 26, 2017, 10:00 AM), https://www.zdnet.com/article/stingray-security-flaw-cell-networks-phone-tracking-surveillance [https://perma.cc/B7TY-LDQV].

50. Zetter, *supra* note 45; *see also* Newman, *5G Is Here*, *supra* note 47 (explaining that "carriers are mostly leaving this data in the clear and at risk for manipulation" or attacks); Rafia Shaikh, *2G Was Too Weak? Turns Out 3G & 4G Networks Are Also Prone to Stingray Surveillance Attacks*, WCCFTECH (July 26, 2017 3:36 PM), https://wccftech.com/3g-4g-lte-stingray-surveillance/ [https://perma.cc/3EQ2-V5TG].

51. *How Secure is Your Cellphone Provider?*, UPGUARD (Aug. 5, 2020), https://www.upguard.com/blog/how-secure-is-your-cell-phone-provider [https://perma.cc/AE33-QUYX] (explaining that "[t]he habit of security must be practiced to stay effective" and keep devices safe against attacks). 6G, with its terahertz (extremely high-frequency wavelength located between microwave and infrared) data communications networks, is due to launch within a decade and promises to provide even more reliability

Asia, and North America, however, build their systems with the aforementioned protections.[52]

Stingrays release the phone by rejecting the transmission, but phone disruption occurs when the release is not immediate, which is often the case.[53] 2G wireless protocols do not support authentication to cell towers.[54] This vulnerability allows Stingrays to impersonate legitimate cell towers.[55] Downgrade attacks are often implemented as part of a MITM, and may be used to enable a cryptographic attack that might not be possible on a more secure system.[56] Although Stingray's jamming capabilities can prevent enemies from performing criminal acts, such as remote cellphone bomb detonation,[57] jamming "poses potential issues during emergency situations, like, for example, the inability to call 911" or engage in other legitimate time-sensitive communications.[58] Further, such attacks could rapidly drain the cellphone battery.[59] The Federal Communications Commission ("FCC") has the

---

and latency reduction than 5G. The narrow, directional terahertz beam vows to thwart MITM interceptions, but it is premature to make speculations. Patrick Nelson, *5G and 6G Wireless Technologies Have Security Issues*, INSIDERPRO (Oct. 25, 2018), https://www.idginsiderpro.com/article/3315626/5g-and-6g-wireless-technologies-have-security-issues.html [https://perma.cc/Q26Y-K77P].

52. Newman, *5G Is Here*, *supra* note 47 (explaining that "[o]ut of 30 carriers the researchers evaluated in Europe, Asia, and North America, 21 offered connections that were vulnerable to downgrading attacks. Only nine elected to build their systems for launching security protections earlier in the connection process").

53. Zetter, *supra* note 45.

54. *Id.*

55. *Id.*

56. Lily Hay Newman, *5G is More Secure Than 4G and 3G — Except When It's Not*, WIRED (Dec. 15, 2019, 7:00 AM), https://www.wired.com/story/5g-more-secure-4g-except-when-not/ [https://perma.cc/57FH-RTXM].

57. *Id*.

58. Zetter, *supra* note 14; *see also* Zach Whittaker, *Stingray Cell Phone Surveillance Devices May Interfere with 911 Calls, Senator Says*, TECHCRUNCH (Aug. 8, 2018, 10:07 AM), https://techcrunch.com/2018/08/28/stingray-cell-phone-surveillance-devices-may-interfere-with-911-calls-senator-says/ [https://perma.cc/MUJ2-SQMM]. "Stingrays force cell phones in range to transmit information back at 'full signal, consuming battery faster,'" posing similar legitimate dangers in emergency situations. *See* Zachary Pfefferkorn, *This Is What You Need to Know About "Stingrays," The Secret Device That's Stealing Your Phone Data*, THOUGHT CATALOG (Sept. 9, 2014) (internal quotation marks omitted), https://thoughtcatalog.com/zachary-pfefferkorn/2014/09/this-is-what-you-need-to-know-about-stingrays-the-secret-device-thats-stealing-your-phone-data/ [https://perma.cc/K2D6-RMU2]. For example, a person in the area of Stingray surveillance may need to make an emergency call but may find the battery dead due to the Stingray's operation. *See* Mallory Locklear, *Senator asks FCC if Stingrays can interfere with 911 calls*, ENGADGET (June 27, 2018), https://www.engadget.com/2018-06-26-senator-fcc-stingray-interfere-911-calls.html [https://perma.cc/9QG2-Y3F2] (explaining that "[t]he FCC has an obligation to ensure that surveillance technology which it certifies does not interfere with emergency services or the mobile communications of innocent Americans who are in the same neighborhood where law enforcement is using a cell-site simulator").

59. Newman, *5G Is Here*, *supra* note 47. A similar MITM attack can block devices from entering a Power Saving Mode ("PSM"). A PSM is triggered once a device has a stable network connection. The PSM is trigged by the network, which sends a message to stop the

authority to enforce the regulation of Stingrays but has not yet responded to complaints regarding their use.[60]

The International Mobile Equipment Identity ("IMEI") number identifies the handset's number and remains constant even if the SIM card is changed.[61] Once the government obtains the IMSI, it can either ask the third-party carrier to voluntarily disclose the IMEI of a particular phone or compel the carrier under a court order to reveal the identity of the target.[62] The Fourth Amendment's protections, however, may limit the collection of this information.

III. BACKGROUND FOURTH AMENDMENT LAW

The Fourth Amendment safeguards against the government's use of general warrants to conduct broad and indiscriminate searches and any government conduct that constitutes an unreasonable search or seizure.[63] There are two distinct tests that the Court uses to determine

---

cellphone from scanning for cell connectivity, trying to reconnect. Reconnection scanning is a quick battery drain for these devices and can be manipulated to suppress the PSM message trigger, even when exposed in 5G. When these messages are suppressed by this attack, the device's battery will drain "five times faster than if it were in power saving mode — a potential safety issue for embedded devices like sensors or controllers." *Id.*

60. *See What We Do*, FCC, https://www.fcc.gov/about-fcc/what-we-do [https://perma.cc/YH9M-ZT7Q]; *see also* Ernesto Falcon, *FCC Helped Create the Stingray Problem, Now It Needs to Fix It*, ELEC. FRONTIER FOUND. (Oct. 6, 2016), https://www.eff.org/deeplinks/2016/08/fcc-created-stingray-problem-now-it-needs-fix-it [https://perma.cc/U2FL-A3QQ] (explaining that the FCC approved commercial sales of Stingrays to law enforcement); *see also* Cyrus Farivar, *Senator to FCC: How Much do Police Stingrays Drain a Cell Phone Battery?*, ARSTECHNICA (June 26, 2018, 5:00 AM), https://arstechnica.com/tech-policy/2018/06/senator-to-fcc-what-do-you-know-about-stingrays-ability-to-disrupt-911-calls [https://perma.cc/DV7M-MF3Z]. Legislators have asked the FCC for certified, detailed explanations of Stingray testing results but have not yet received them. *See id.*; *see also* Locklear, *supra* note 58 (explaining that Senator Wyden requested information regarding "testing [or lack thereof] conducted by or required by the FCC regarding the disruption of communications"); Dell Cameron, *Lawmakers Urge FCC to Act on Reports of Illegal 'Stingrays' Surveilling US Capital*, GIZMODO (Apr. 5, 2018, 5:23 PM), https://gizmodo.com/lawmakers-urge-fcc-to-act-on-reports-of-illegal-stingra-1825027480 [https://perma.cc/U5QQ-G65C] (explaining that House Representatives Frank Pallone, Jr., Eliot Engel, and Bennie Thompson urged the FCC to take immediate steps to halt suspected illegal use of Stingrays. The FCC formed a Stingray task group but generated no solutions and stopped regularly meeting).

61. Jen Manso, *Cell-Site Location Data and the Right to Privacy*, 27 SYRACUSE J. SCI. & TECH. L. 1, 4 n.15 (2012). A cellphone has two identifiers: (1) the IMSI (International Mobile Subscriber Identity) number, which reveals the user's country code, user account, network code, and telephone number; and (2) the IMEI (International Mobile Equipment Identity) number which identifies the handset's number and remains constant even if the SIM card is changed. Ghayas, *supra* note 43.

62. Ghayas, *supra* note 43.

63. Gray, *supra* note 32; Davies, *supra* note 32 (noting that "the Framers preferred use of specific warrants rather than warrantless intrusions" and wanted to prevent "unjustified searches and arrests from occurring").

whether a search under the Fourth Amendment has occurred: the property-based approach of *United States v. Jones* and the privacy-based test of *Katz v. United States*.[64] Privacy expectations protected by the Fourth Amendment have been limited by the third-party doctrine, which provides that an individual sometimes cannot assert Fourth Amendment protection in information that he voluntarily provided to another entity.[65] The Supreme Court recently limited the third-party doctrine with respect to digital information in *Carpenter v. United States*.[66] The Fourth Amendment's property and privacy principles lay the groundwork for analysis of the use of new technology, including CSS, such as Stingrays.[67]

A. Property-based Approach

Courts typically apply the property-based approach first, if possible.[68] This approach protects a person's house, papers, and effects, as provided for in the Fourth Amendment.[69] When the government obtains information by physically trespassing on that property, the government has undoubtedly conducted an illegal search within the original meaning of the Fourth Amendment.[70]

In *Olmstead v. United States*, the government surreptitiously tapped the phone of suspects by placing wiretaps on public streets near homes to avoid entering the private property itself.[71] The Court held that wiretaps attached to telephone wires on public streets did not constitute a search under the Fourth Amendment.[72] Justice Brandeis dissented, noting that the Fourth Amendment should be read to prohibit

64. *See* Katz v. United States, 389 U.S. 347, 359 (1967); United States v. Jones, 565 U.S. 400, 404–05 (2012).

65. *See* Smith v. Maryland, 442 U.S. 735, 740–41 (1979) (finding no legitimate expectation of privacy in phone records for the numbers customers have dialed); United States v. Miller, 425 U.S. 435, 448–49 (1976) (finding no reasonable expectation of privacy when customers voluntarily give any information contained in bank records to the bank and such records are observable by the bank's employees).

66. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); *see also* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 358, 363 (2019).

67. *See Jones*, 565 U.S. at 404–09; *see also* United States v. Sweeney, 821 F.3d 893, 899 (7th Cir. 2016) (finding that there are two different approaches that courts use to determine whether a police officer's actions constitute a search under the Fourth Amendment — a property-based and a privacy-based approach).

68. Florida v. Jardines, 569 U.S. 1, 11 (2013) (noting that it is unnecessary to apply the privacy-based approach if a violation of the Fourth Amendment has been found under the property-based approach).

69. U.S. CONST. amend. IV.

70. *Jardines*, 569 U.S. at 5.

71. Olmstead v. United States, 277 U.S. 438, 455–57.

72. *Id.* at 464.

"every unjustifiable intrusion by the Government upon the privacy of the individual."[73]

In *Katz*, the Court overruled *Olmstead*'s property-based approach as inadequate to protect against technological intrusions, echoing Justice Brandeis's dissent.[74] *Katz* expanded the Fourth Amendment's protection to include legitimate privacy expectations even if law enforcement did not a commit a trespass to acquire the information.[75] Although *Katz* rejected the *Olmstead* property-based approach, a modern property-based approach has recently emerged.[76]

In *Jones*, the Court revived the property-based analysis to determine whether a search occurred under the Fourth Amendment. There, the government installed a GPS tracking device on a vehicle and monitored it for twenty-eight days.[77] The Court held that the warrantless installation of a GPS tracking device on a vehicle constituted a search under the Fourth Amendment.[78] Writing for the Court, Justice Scalia noted that the installation was a physical trespass of the vehicle.[79] Five Justices wrote or joined separate opinions concurring in the judgment, reasoning that "surreptitious long-term monitoring of the vehicle also impinged on reasonable expectations of privacy, even if those movements were in public view."[80]

Property rights are not the lone measure to determine a violation of privacy.[81] Courts also look to the privacy-based approach to determine whether the actions of law enforcement constitute a search under the Fourth Amendment.

---

73. *Id.* at 478 (Brandeis, J., dissenting); *see also* Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting) (noting that "the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment").

74. Katz v. United States, 389 U.S. 347, 348 (1967).

75. *Id.*

76. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012); Florida v. Jardines, 569 U.S. 1, 7–8 (2013).

77. *Jones*, 565 U.S. at 403.

78. *Id.* at 404.

79. *Id.*

80. *Id.* at 415 (Sotomayor, J., concurring); *id*. at 430 (Alito, J., concurring); *see also* Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 216 (2018).

81. Soldal v. Cook County, 506 U.S. 56, 64 (1992) (noting that property rights "are not the sole measure of Fourth Amendment violations").

B. Privacy-based Approach

Current Supreme Court doctrine does not undermine or substitute the *Katz* privacy-based approach with the *Jones* property-based approach.[82] Instead, the Court will find an illegal search if one exists under either approach.[83] The privacy-based approach recognizes that Fourth Amendment protections also extend to areas where a person has a reasonable expectation of privacy, assuming that expectation is one that society is willing to recognize.[84] Instead of relying on the trespass doctrine, *Katz* redefined Fourth Amendment protections, creating "a more flexible reasonable expectation of privacy test that protected against government intrusion, physical or otherwise, so long as the targeted individual intended to keep his affairs private."[85] *Katz* involved the government's use of an electronic listening device to eavesdrop on the defendant's conversations within an enclosed public telephone booth.[86] The Court reasoned that despite a phone booth's public accessibility, "it is a temporarily private place whose momentary occupants' expressions of freedom from intrusion are recognized as reasonable."[87] Under the two-prong test that Justice Harlan articulated in his concurrence, a search takes place when (1) the individual manifests an actual expectation of privacy that (2) society is willing to recognize as legitimate, justifiable, or reasonable.[88]

---

82. George C. Thomas III, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 TEX. TECH L. REV. 199, 223–25 (2010) (discussing the property-based trespass doctrine and the privacy-based approach); *see also, e.g.*, *Jones*, 565 U.S. at 404–10. Justice Alito and Justice Gorsuch both criticized *Katz* in their *Carpenter* dissents. Carpenter v. United States, 138 S. Ct. 2206, 2236–46 (2018) (Alito, J., dissenting); *id.* at 2264–69 (Gorsuch, J., dissenting); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004) (arguing that the *Katz* "reasonable expectation of privacy" test has "not substantially changed the basic property-based contours of Fourth Amendment law").

83. *See* United States v. Sweeney, 821 F.3d 893, 899 (7th Cir. 2016).

84. *See* Florida v. Jardines, 569 U.S. 1, 5–6; Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

85. Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, 138 (2018) (citing *Katz*, 389 U.S. at 362).

86. *Katz*, 389 U.S. at 348 (majority opinion).

87. *Id.* at 361 (Harlan, J., concurring).

88. Courts have consistently used the *Katz* two-prong test to assess the government's surveillance of suspects in cases of aerial surveillance (Florida v. Riley, 488 U.S. 445, 454 (1989); California v. Ciraolo, 476 U.S. 207, 207 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 230 (1986)), videotape surveillance (United States v. Leon Davis, 326 F.3d 361, 365 (2d Cir. 2003)), searches of curbside trash (California v. Greenwood, 486 U.S. 35, 39–40 (1988)), canine sniffs (*Jardines*, 569 U.S. at 5; United States v. Place, 462 U.S. 696, 720 (1983)), chemical field tests (United States v. Jacobsen, 466 U.S. 109, 112–13 (1984)), file access through peer-to-peer file sharing (United States v. Borowy, 595 F.3d 1045, 1047 (9th Cir. 2010)), and location tracking of airplanes (United States v. Butts, 729 F.2d 1514, 1516 (5th Cir. 1984)), and cars (United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010)). *See also* Orin S. Kerr, *Four Models of Fourth Amendment Protection,* 60 STAN. L. REV. 503, 503 (2007); David Gray, *The Fourth Amendment Categorical Imperative,* 116

In *Kyllo v. United States*, the police used a thermal-imaging device to detect heat emanating from the high-intensity lamps used to grow marijuana plants while standing outside of the defendant's home.[89] The device revealed that part of the house was significantly hotter than the rest.[90] The police used this information to obtain a warrant.[91] Justice Scalia, writing for the Court, stressed that any details inside a home are intimate and protected by the Fourth Amendment, requiring a warrant unless they are freely observable by the public.[92]

Private information stored on a digital device outside the home may also be subject to Fourth Amendment protection. In *Riley v. California*, the Court found the warrantless access of an arrestee's cellphone data as a search incident to a lawful arrest and unanimously held that the government must obtain a warrant previous to such a search.[93] The *Riley* Court noted that the cellphone is a unique device and considered cellular phones to be fundamentally different than other types of personal property that are discovered in searches incident to arrest because of the comprehensive nature of the information stored within.[94] Further, the Court considered that cellphones store sensitive personal information, including browser history and Cloud data, that far surpasses physical records both quantitatively and qualitatively in the amount of

---

MICH. L. REV. 14, 15 (2017) ("The reasonable expectation of privacy test has granted government agents unfettered discretion to engage in a wide variety of search activities completely free of Fourth Amendment regulation."). A person's home is a location where both the individual and society recognizes a reasonable expectation of privacy. But the Court has found that "objects, activities, or statements [exposed] to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited." *Katz*, 389 U.S. at 361; s*ee also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that there is no legitimate expectation of privacy in one's records of phone calls held by one's phone company); United States v. Miller, 425 U.S. 435, 441–43 (1976) (holding that there is no legitimate expectation of privacy in one's financial records held by one's bank); Couch v. United States, 409 U.S. 322, 335 (1973) (holding that there is no legitimate expectation of privacy in one's financial and tax records held by one's accountant); Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that there is no legitimate expectation of privacy in statements made to confidential informant); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) [hereinafter Kerr, *A User's Guide*].

89. 533 U.S. 27, 40 (2001) (finding that the use of a thermal imaging device (FLIR) from a public vantage point to monitor the radiation of heat from a person's home was a "search" within the meaning of the Fourth Amendment, and thus required a warrant).

90. *Id.* at 39.

91. *Id.* at 27.

92. *Id.* at 40.

93. Riley v. California, 573 U.S. 373, 402–03 (2014).

94. *Id.* The Court also reasoned that a cellphone search furnishes the government with far more information than could be secured in the search of a home, explaining that "the phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." R. Craig Curtis, Michael C. Gizzi, & Michael J. Kittleson, *Using Technology the Founders Never Dreamed of: Cellphones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 75 (2014) (quoting *Riley*, 573 U.S. at 396).

potentially accessible data.[95] Finally, the Court noted the government's ability to use a cellphone's GPS capability to precisely track an individual's contemporaneous and historic location data "not only around town but also within a particular building," which could "reconstruct someone's specific movements down to the minute."[96]

The *Katz* approach provided an amorphous Fourth Amendment framework; seeking to clarify the standard, the Court has complicated the doctrine through "rules, exceptions, and exceptions to the exceptions,"[97] including the third-party doctrine, in which "an individual has no legitimate expectation of privacy in information provided to third parties."[98]

C. Third-Party Doctrine

Under the third-party doctrine, voluntarily sharing information forfeits one's right to a reasonable expectation of privacy.[99] For example, banks know what customers purchase through credit card paper trails and phone companies know the numbers users call from their phone records.[100] When the government searches these banks or phone companies for a customer's information, the third-party doctrine prohibits the customers from asserting a Fourth Amendment claim.[101] The Court first recognized the third-party doctrine in *United States v. Miller*.[102] In *Miller*, the Court held that a defendant had no right to privacy in his banking records, because they were business records belonging to the bank.[103] In *Smith v. Maryland*, the Supreme Court held that police did not require a warrant to use a pen register to monitor a suspect's outgoing call data, noting that the "petitioner voluntarily conveyed numerical information to the telephone company."[104] *Miller* and *Smith*

95. *Riley*, 573 U.S. at 395–96 ("An Internet search and browser history . . . could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

96. *Id.*

97. Donahue, *supra* note 5, at 347.

98. Hu, *supra* note 85, at 138–39 (quoting ACLU v. Clapper, 959 F. Supp. 2d 724, 749 (S.D.N.Y. 2013)).

99. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (records of phone calls held by phone company); United States v. Miller, 425 U.S. 435, 443 (1976) (financial records held by bank); Couch v. United States, 409 U.S. 322, 335 (1973) (financial and tax records held by accountant); *see also* Kerr, *A User's Guide*, *supra* note 88, at 1210.

100. *See Miller*, 425 U.S. at 432; *Smith*, 442 U.S. at 735.

101. *Smith*, 442 U.S. at 735 (holding that there is no legitimate expectation of privacy in phone records for the numbers customers have dialed); *Miller*, 425 U.S. at 443 (holding no reasonable expectation of privacy when customers voluntarily give any information contained in bank records to the bank and such records are observable by the bank's employees).

102. 425 U.S. at 443.

103. *Id.*

104. *Smith*, 442 U.S. at 744.

"established and applied the legal principle that when an individual voluntarily gives information to a third party, the privacy interest in that information is forfeit[ed]."[105]

In *Carpenter v. United States*, the Court considered whether the government could conduct a warrantless search and seizure of seven or more days of cell-site location information ("CSLI") from cellphone companies.[106] After law enforcement arrested four men suspected of robberies, one suspect disclosed the identities of his accomplices and their cellphone numbers.[107] The government obtained records, spanning 127 days of defendant's location data, from third-party cellphone service providers.[108] In a 5-4 decision, the Court rejected reliance on the third-party doctrine, holding that the acquisition of CSLI of seven or more days constitutes a search under the *Katz* test.[109] The Court noted that cell-site records should not be subject to the third-party doctrine because it would be an intrusion into a private sphere as those records have a unique and revealing nature.[110] *Carpenter* has clarified that the third-party doctrine acts as a factor to diminish the reasonable expectation of privacy but does not necessarily extinguish it.[111] The government's use of compelled disclosure to obtain records from a third party, or the target, does not foreclose a reasonable expectation of privacy inquiry concerning those records.[112]

This effects framework could also readily incorporate other doctrines of property law. For example, courts could treat data and other technological information stored with a third party as a bailment. In his *Carpenter* dissent, Justice Gorsuch expressed support for the use of bailment law in Fourth Amendment analysis. Under common law, bailment is a non-ownership transfer of possession.[113] In a bailment, the

105. Sabrina McCubbin, *Summary: The Supreme Court Rules in* Carpenter v. United States, LAWFARE (June 22, 2018, 2:05 PM), https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states [https://perma.cc/8PJP-2U8Z].

106. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (holding that a warrant is required for police to access cell-site location information (CSLI) from a cellphone company). CSLI is the detailed geolocation information generated by a cellphone's communication with cell towers. *Id.*

107. *Id.* at 2212.

108. *Id.*

109. *Id.* The *Carpenter* Court found that, under the Fourth Amendment, an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. *Id.* at 2222. The Court noted, however, that in some instances, exigencies may support a warrantless search of an individual's cell-site records. *Id.* (citing Kentucky v. King, 563 U.S. 452, 460 (2011)).

110. *Carpenter,* 138 S. Ct. at 2217. An intrusion into a "private sphere" as articulated in *Katz* occurs when "an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable.'" *Id.* at 2206–07.

111. *Id.* at 2206.

112. *See id.* at 2247 (Alito, J., dissenting).

113. *See* JOSEPH STORY, COMMENTARIES ON THE LAW OF BAILMENTS 4 (1846) (defining bailment as "a delivery of a thing in trust…upon a contract, express or implied, to conform to the object of purpose of the trust"); 8 C.J.S. Bailments § 1 n.3 (denoting a bailment, in its

owner, or bailor, transfers physical possession of personal property to a bailee for a time but retains ownership.[114] The bailee holds the personal property in trust and delivers the property back to the bailor when the purpose is accomplished.[115] The bailee thus owes a legal duty to safeguard the property. Fourth Amendment protections, Justice Gorsuch argued, "do not automatically disappear just because you share [your papers and effects] with third parties:"[116] In other words, entrusting others with your property does not give them carte blanche to use it for any purpose. In fact, a bailee who uses the item against the bailor's instructions is liable for conversion.[117] Although the Court did not take up Justice Gorsuch's implied invitation to revisit the third-party doctrine, the Court's refusal to apply it to extinguish the expectation of privacy in *Carpenter* illustrates its now diminished role. The Court today has a more conservative composition than it did when it decided *Carpenter*. One would ordinarily expect this to mean that the Court will trend towards a pro-government, less expansive view of the Fourth Amendment. Justices Kavanaugh and Barrett, however, are self-professed Originalists and it remains to be seen whether this approach will lead to more robust Fourth Amendment protections as it did in many opinions authored by Justice Scalia and now Justice Gorsuch.[118]

The Founders were concerned with the extent of government power and reach, and sought to place a limit on the government's police power after being subjected to colonial rule under the Crown.[119] *Carpenter*'s test and reasoning resonates much more directly with the

---

ordinary legal meaning, as "a contract resulting from delivery of a thing by the bailor to the bailee on condition that it be restored to the bailor in accordance with his or her directions as soon as the purpose for which it was bailed is satisfied").

114. *Bailment*, BLACK'S LAW DICTIONARY (11th ed. 2019).

115. *Id.*

116. Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).

117. *Id.* at 2269 (citing 8 C.J.S. Bailments § 43 (2017)).

118. *See, e.g.*, United States v. Jones, 565 U.S. 400, 404–09 (2012) (using the property approach and finding a Fourth Amendment violation); Florida v. Jardines, 569 U.S. 1, 5 (same); United States v. Knotts, 460 U.S. 276, 286 (1983) (same).

119. The Court's treatment of the Fourth Amendment as a limit on government power rather than a protection of an unenumerated right to privacy also accords with the structure of the Bill of Rights securing liberties through restraints on government action. Orin Kerr would call this "equilibrium-adjustment": When government power grows, the Court moves the Fourth Amendment line to prevent arbitrary encroachment. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011) [hereinafter Kerr, *An Equilibrium-Adjustment*]. That would explain the move from *Olmstead* to *Katz*, *see id.* at 514–15, the holding in *Kyllo*, *see id.* at 496, and the refusal to apply *Smith* and *Miller* in *Carpenter*, *see* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/W234-3VEU] (noting that "[o]ld rules don't apply" due to equilibrium-adjustment).

Founders' objective that the Fourth Amendment serve as a restriction on government power, not just as a protection of privacy.[120]

IV. STINGRAY INTERFERENCE WITH CELLPHONES

A Stingray, by design, interferes with the use of cellphones during its operation of gathering location information. The Court has already recognized a higher reasonable expectation of privacy in cellphones, noting that Cloud storage raises "the possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee."[121] Modern cellphones, with vast potential storage on the device itself and in the Cloud, provide a plethora of data to anyone who can open it with a password or biometric scan. Due to this extensive reach, searches of these modern devices are quantitatively different from searches of mailboxes limited by physical restraints.[122] Moreover, the "government can store [this data] and efficiently mine them for information years into the future."[123] And, as Justice Sotomayor reasoned in her concurrence in *Jones*, modern phones offer unique insights into an individual's past, providing a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[124]

Justice Sotomayor's concerns are even more relevant today where many current cellphones have hundreds of gigabytes of storage on the device itself, without even considering Cloud storage.[125] The Court acknowledged this privacy concern in *Riley*, where it unanimously held that the search of the phone did "not justify dispensing with the warrant requirement" even under the search incident to arrest exception.[126] This exemplifies the high degree of privacy in a cellphone. A Stingray is used to locate suspects, and searching a cellphone for location data

120. Ohm, *supra* note 66, at 390 (citing *Carpenter*, 138 S. Ct. at 2207 (noting that "the Amendment seeks to secure 'the privacies of life' against 'arbitrary power' . . . a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance'").

121. Riley v. California, 573 U.S. 373, 375 (2014). "[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 385.

122. *See Ex parte* Jackson, 96 U.S. 727, 733 (1878) (drawing a distinction between letters and sealed packages, which cannot be inspected without a warrant, and newspapers and magazines, which are "purposely left in a condition to be examined").

123. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

124. *Id.*

125. IPHONE, https://www.apple.com/iphone/ [https://perma.cc/4B5Y-36FL]; *see also* Richard Goodwin, *How Much iPhone Storage Do You REALLY Need?*, KYM (Mar. 4, 2020, 10:52 AM), https://www.knowyourmobile.com/user-guides/how-much-iphone-storage-do-you-really-need [https://perma.cc/BZ97-RGL8] (explaining that iPhones have storage tiers from 32 to 512 gigabytes).

126. *See* Riley v. California, 573 U.S. 373, 388 (2014). Prior to *Riley*, the Court had recognized other exceptions to the warrant requirement. *See* United States v. Robinson, 414 U.S. 218, 218 (1973) (holding that a warrant is not required for a search incident to a lawful arrest).

would surely have an even higher burden of acquiring a warrant than in *Riley*.[127] In fact, Justice Sotomayor in her *Jones* concurrence feared that unfettered access to the device-emitted GPS information by law enforcement without a warrant would "chill[] associational and expressive freedoms" and "alter the relationship between citizen and government in a way that is inimical to democratic society."[128] Justice Sotomayor explained that the usual constraints on intrusive law enforcement practices are "limited police resources and community hostility."[129] In the case of cellphone surveillance, however, the relatively low cost of cellphone surveillance prevents limited police resources from serving as a check.[130] Similarly, Justice Sotomayor reasoned that the practice was inherently surreptitious because (1) individuals do not know when surveillance occurs on their phones and (2) communities cannot prevent surveillance of which they are unaware.[131]

The majority in *Carpenter* considered historical precedent, noting that the Framers, at the time of the Founding, aimed to prevent the formation of over-extensive police surveillance.[132] *Carpenter* acknowledged that historical cell-site records trigger even greater privacy concerns than the GPS monitoring considered in *Jones*.[133] The Court noted that "the accuracy of CSLI is rapidly approaching GPS-level precision,"[134] and found that, "[a]ccordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[135] The use of a Stingray to acquire location data from a phone would likely be an even stronger case for Fourth Amendment protection than the use of location data in *Carpenter*. Unlike in *Carpenter*, where law enforcement gathered location data from a third-party provider, the Stingray allows law enforcement to independently gather location data, rendering the third-party doctrine inapplicable.[136] The breadth of Stingray searches and the indiscriminate mass gathering of

127. A Stingray's capability to search for more than merely location data could create even greater privacy concerns.

128. *Jones*, 565 U.S. at 416 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

129. *Id.* (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

130. *Id.* at 415–16.

131. *See id.*

132. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

133. *Id.* at 2218.

134. *Id.* at 2219.

135. *Id.* (citing the Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Petitioners at 12, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (describing triangulation methods that estimate a device's location inside a given cell sector)).

136. *Cf.* Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that a pen register was not a search because the "petitioner voluntarily conveyed numerical information to the telephone company"); United States v. Miller, 425 U.S. 435, 442 (1976) (finding that a bank customer has no expectation of privacy in their bank transactions).

data would also likely persuade a court to deem Stingray tracking a search.

V. WARRANT REQUIREMENT FOR CELLPHONES AS EFFECTS

A cellphone should be considered an effect under the Fourth Amendment. Effects under the Fourth Amendment would originally have been understood to mean personal property.[137] When a Stingray interferes with the cellphone signal, it interferes with a possessory interest in the use of the cellphone. This interference constitutes a search under the property-based approach and thus requires a warrant.

A. Cellphones as Effects

Cellphone ownership is a property right that includes a bundle of possessory interests.[138] The most important interest is the ability to use one's cellphone, including the ability to make calls. Interference with one or more of these possessory interests amounts to a property trespass. A Stingray that interferes with a cellphone's use, therefore, has trespassed upon the cellphone by interfering with both the use of its functions and the owner's right to exclude.

In the same way that the Court applied the trespass test in *Jones*, the Court could apply the trespass test to Stingrays and examine cellphones as effects.[139] In *Jones*, the Supreme Court did not provide a definition of effects. Although the Court has devoted significant effort to refining the rest of its search and seizure rules, it has not clarified how to determine whether something is an effect.[140] The Court found that a parcel,[141] a vehicle,[142] and luggage[143] were undisputedly effects, while "open fields"[144] were not. Yet, the Court held in a footnote that "[t]he Framers would have understood the term effects to be limited to personal, rather than real, property."[145] The Court's footnote concurs with the Founding Era understanding that the Fourth Amendment was meant to protect personal property.[146] The Founders placed great importance

137. Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 1001 (2016).

138. This is often referred to as the "bundle of sticks" conception of property rights. *See* Denise R. Johnson, *Reflections on the Bundle of Rights*, 32 VT. L. REV. 247, 247 (2007).

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

140. Brady, *supra* note 137, at 946.

141. United States v. Jacobsen, 466 U.S. 109, 114 (1984).

142. United States v. Jones, 565 U.S. 400, 404 (2012).

143. United States v. Place, 462 U.S. 696, 705–06 (1983).

144. Hester v. United States, 265 U.S. 57, 59 (1924); Oliver v. United States, 466 U.S. 170, 176 (1984).

145. Brady, *supra* note 137, at 960 (internal quotation marks omitted) (quoting *Oliver*, 466 U.S. at 177 n.7).

146. *Id.* at 981.

on the privacy interests of personal property and thus included the term effects in the Fourth Amendment to protect those interests.[147] Personal property required protection for three reasons. First, the value of the property itself warranted protection. Second, the government invasion of privacy and property interests in the effect's location would be an undue intrusion, absent a warrant. Third, the inherent connection between the constitutional protection against search and seizure and the laws protecting personal property more generally both justify the protection of the personal property.[148] In contrast, privacy precedent has focused solely on places, without examining the personal property rights the Founders wrote the Fourth Amendment to protect.[149] Black's Law Dictionary defines personal property as "[a]ny movable or intangible thing that is subject to ownership and not classified as real property."[150]

As established above, the Founding Era understanding of an effect was equivalent to the common law definition of personal property at the time. Thus, if a court reasonably recognizes an object as personal property, it should deem the object an effect for Fourth Amendment purposes.[151] This approach would better accord the Court's Fourth Amendment jurisprudence with its original personal property understanding.[152] As a test to determine whether an object is personal property, courts could use the Founding Era understanding that personal property was defined by three factors: "(1) the ability to exclude others, (2) the ability to transfer the object, and (3) control over its use."[153] This would allow courts to analyze whether an item constitutes an effect for Fourth Amendment purposes. Courts could then determine if a trespass has occurred by considering whether the government interfered with any of these three factors.

Applying this test to a cellphone, courts would see that an individual is able to (1) exclude others from his phone through encryption, a pass code, or other means;[154] (2) transfer his phone through gift or sale;

---

147. *Id.*

148. *See id.*

149. *Id.*

150. *Id.* at 948 (citing *Property*, BLACK'S LAW DICTIONARY (10th ed. 2014)); *see also Chattel*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining personal property as "movable goods, visible and tangible in their nature, and in the possession either of the owner or of some other person on his behalf").

151. *Id.* at 1001.

152. *Id.* at 1002 (citing Minnesota v. Carter, 525 U.S. 83, 88 (1998)). This approach would also "fit the Supreme Court's directive that Fourth Amendment law is constructed by the 'concepts' and 'understandings' that derive from social life and myriad state laws." *Id.*

153. *Id.*

154. When Stingrays collect data from the cellphone that the cellphone owner does not intend to share, it violates the owner's right to exclude. This would also constitute a trespass because the right to exclude is the keystone property right and surreptitious data collection would violate that right.

and (3) control the use of his phone by using apps, texting, or calling. Courts could then find a Fourth Amendment search under the trespass theory if the government interfered with any of the property rights associated with the phone. Courts routinely recognize these personal property rights and should apply these principles in their Fourth Amendment jurisprudence.

Courts could apply the trespass test to potential effects by asking:

> (1) is this effect the sort of item that someone owns; and (2) would an outside observer recognize that the item is not abandoned, or in other words, does its owner have a reasonable expectation of privacy?[155] If both inquiries are answered in the affirmative, courts can proceed to examine (3) whether the challenged government behavior was a trespass in that it violated the owner's expectations that the item would remain undisturbed in that manner, and (4) whether any exigency exceptions apply.[156]

First, as described above, the appropriate effect for the Fourth Amendment analysis is the cellphone itself, which a person typically owns. Second, an outside observer would recognize that a cellphone in someone's possession, even if not in use, has clearly not been abandoned. Third, the use of a Stingray may disturb the owner's possessory rights in the cellphone by trespassing to gain private location data. This interference violates the owner's expectation of undisturbed control over his cellphone. Although this disruption may seem to only trespass upon the cellphone signal and not the cellphone itself, the disruption interferes with the key use of the cellphone, making calls. It therefore intrudes upon the effect of the phone because the possession of the phone includes the right to use it. Worse, the Stingray use potentially infringes upon the expectation that the phone can be used to dial 911 during an emergency through the downgrade attack, discussed in Part II.[157] Finally, courts will have to determine on a case-by-case basis whether

---

155. Brady, *supra* note 137, at 996–97. The term "owner" may be somewhat misleading as a person may have a Fourth Amendment right in "something he or she possesses only temporarily." *Id.* at 997 n.228.

156. *Id.* at 996–97.

157. *See supra* Part II. Stingrays sweep data and disrupt cellular service "for any phone in their vicinity — not just targeted phones." Zetter, *supra* note 45. FBI agent Michael A. Scimeca disclosed the disruptive capability, stating that "its use has the potential to intermittently disrupt cellular service to a small fraction of Sprint's wireless customers within its immediate vicinity." *Id. See* David Kravets, *Justice Department's Warrantless Spying Increased 600 Percent in Decade*, WIRED (Sept. 27, 2012, 6:19 PM), https://www.wired.com/2012/09/warrantless-surveillance-stats/ [https://perma.cc/9EA6-82WT].

any exigency exceptions apply to a Stingray's use. Absent any exigency, the warrantless use of a Stingray violates the Fourth Amendment.

One may object and instead argue that the relevant target of the search is in fact the data itself and not the cellphone. If the relevant target were the data, then who owns it? Is the data the personal property of the cellphone owner, the phone company, or the Cloud where it may be stored? Such inquiries are unnecessary in this instance. A Stingray targets and disrupts a cellphone's ability to work, and only then extracts the data. To better illustrate this proposition, consider the search of a home. In Fourth Amendment jurisprudence, when the government conducts a search of a home to search for things within the home, like contraband, a warrant is issued for the search of the home.[158] Similarly, when the government uses a Stingray to conduct a search of one's phone, to ultimately search for things within the phone, a warrant should be likewise issued. In other words, someone's home is targeted when searched, and the contraband, ultimately extracted. Likewise, the target of the Stingray is the cellphone itself, even if its data is ultimately extracted.

If the Stingray catches a signal that the phone routinely broadcasts, but does not otherwise interfere with the cellphone, would that be considered a trespass? In the case of GPS data, the Stingray is not intruding into the phone and extracting location information, but rather collecting the pings to the Stingray itself. Courts could analyze such new technology with a property-based approach, instead of the *Katz* reasonable expectation of privacy. This new approach could view any interference with a cellphone's key functions as a trespass due to the degradation of the property that such interference would cause. In *Jones*, for example, the majority opinion did not consider whether the *Katz* reasonable expectation of privacy test applied to warrantless GPS tracking.[159] Justice Scalia, writing for the Court relied on a property-based trespass theory, as "an alternative to *Katz*."[160] The Court held that the defendant's vehicle was an effect and that the government's physical trespass upon it, through the GPS tracker, constituted a search subject to the Fourth Amendment.[161] Justice Scalia further explained that a property-based

158. Kyllo v. United States, 533 U.S. 27, 31 (2001) (noting that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no").

159. Hu, *supra* note 85, at 130 (citing United States v. Jones, 565 U.S. 400, 411 (2012) ("For unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.")).

160. *Id.*

161. *Jones*, 565 U.S. at 404–05 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion

approach to Fourth Amendment protection does not change based on the publicness of the location.[162] Instead, the Fourth Amendment may limit the invasion of a personal-property interest to obtain information regardless of where that property is located.[163] A Stingray search, therefore, may be unreasonable as a trespass to an effect, even if it occurs in public.

B. Warrant Requirement

The Court has recognized a number of exceptions to the Fourth Amendment's warrant requirement.[164] These exceptions leave most searches and seizures to the discretion of law enforcement officers in the first instance.[165] Generally, exceptions are based on less invasive privacy interests and administrative expediency, neither of which apply to Stingrays.[166] At the same time, the Court has expanded the immunity function of warrants by barring civil actions where officers violate the Fourth Amendment in good faith.[167]

The Founders could not have known about nascent technology, such as the thermal imaging devices in *Kyllo* or Stingrays here, and therefore did not contemplate how such technology would impact privacy.[168] The text and original public meaning of the Fourth Amendment, however, are not limited merely to technologies in existence at the time. The relevant inquiry concerns not what the Founders thought about thermal imaging devices or Stingrays, but instead the Founding Era public understanding of the term effects. This understanding can

---

would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

162. *Id.* at 406. In contrast, the publicness of the location can diminish the reasonable expectation of privacy under the privacy-based approach. *See* Oliver v. United States, 466 U.S. 170, 179 (1984) (finding no societal interest in protecting privacy in areas of open view to the public); Hester v. United States, 265 U.S. 57, 57 (1924) (finding that the special protections afforded by the Fourth Amendment does not extend to open fields).

163. *See Jones*, 565 U.S. at 408.

164. California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring) (describing the warrant as "basically unrecognizable" due to all the exceptions); United States v. Place, 462 U.S. 696, 721 (1983) (Blackmun, J., concurring); Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1475 (1985) (explaining that more searches are performed pursuant to an exception than to a warrant).

165. *See, e.g.*, Kentucky v. King, 563 U.S. 452, 473 (2011) (Ginsburg, J., dissenting) ("In lieu of presenting their evidence to a neutral magistrate, police officers may now knock, listen, then break the door down, never mind that they had ample time to obtain a warrant.").

166. Exceptions to the Fourth Amendment's warrant requirement include, but are not limited to: search incident to lawful arrest, items in plain view, consent, *Terry* stops (stop-and-frisk), automobile exception, hot pursuit, exigent circumstances, and open fields.

167. United States v. Leon, 468 U.S. 897, 925–26 (1984) (establishing the good faith exception in the suppression context).

168. Kyllo v. United States, 533 U.S. 27, 46 (2001) (Stevens, J., dissenting) ("It is hard to believe that [concealing the heat escaping from one's house] is an interest the Framers sought to protect in our Constitution."); Gray, *supra* note 32, at 466.

then be applied to technologies not in existence at the time without the need to engage in imaginative reconstruction concerning how the Founders would have viewed the technology itself.

The government has increasingly relied on modern surveillance technology, bringing the importance of the warrant requirement to public attention.[169] As technology advances, novel issues arise. Surreptitious surveillance, like the thermal imaging device in *Kyllo*, and Stingrays today, can infringe upon a person's privacy without even allowing him notice of this violation. Without a warrant, law enforcement could use that technology with unfettered access. In such a case, no one would know the extent of the government's surveillance.[170] Writing for the Court, Justice Scalia noted that a remedy was needed to safeguard people from the technological threats of "more sophisticated systems that are already in use or in development."[171] Justice Scalia's reasoning in *Kyllo* is consistent with the Framers' original reasoning for imposing the warrant requirement, namely to check excessive government surveillance.[172] This understanding of the warrant requirement underscores its importance in the Stingray context.

Virtual intrusions may seem to be a tenuous fit in the warrant requirement framework, which has primarily addressed physical intrusions constituting more traditional trespasses to real property.[173] Stingray searches, however, are better examined as trespasses to effects, placing effects on par with the other categories enumerated in the Fourth Amendment, persons, papers, and houses.[174] Furthermore, a property-based framework would cure the anomalous results caused by analyzing virtual searches under the privacy-based framework. By adding protections for effects in circumstances where they may be unprotected, such as remote searches, digital searches would be subject to the same limitations as physical searches. The property-based framework would also fit in with the Court's current trespass test framework as outlined in *Jones*.[175]

---

169. *See, e.g.*, Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015), http://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html?hpid=z1 [https://perma.cc/V3QQ-FWRL] (explaining how Stingray works).

170. Gray, *supra* note 32, at 466 (citing *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'")).

171. *Kyllo*, 533 U.S. at 36.

172. *See* Gray, *supra* note 32, at 458.

173. *Id.* (citing *Kyllo*, 533 U.S. 27 at 36) (noting that "it is hard to imagine anything more unsettling or disruptive to the domestic sanctity of the home and its inherent intimacy."); *see also* 533 U.S. at 37–38 ("In the home . . . all details are intimate details, because the entire area is held safe from prying government eyes.").

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

175. United States v. Jones, 565 U.S. 400, 404–06 (2012).

A revival of the original meaning of effects would not only protect the civil liberties implicated by the use of Stingrays, but also clarify other areas of Fourth Amendment law. Clearly defining effects as a distinct but equally protected category would properly allow the Fourth Amendment to protect them on the same level as "persons, papers, and houses."[176] For example, under current doctrine, if the government obtains a warrant for the search of a cellphone and remotely searches the defendant's Cloud drive, it remains unclear whether the remote search requires a separate warrant. The Court could recognize the Cloud access itself as another search of a different effect, namely the Cloud drive, requiring a separate warrant, without the need to arbitrarily analyze the reasonableness of that access.[177] This understanding accords with the reasoning behind the majority's statement that the search in *Riley* was constitutionally impermissible because of "[t]he possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee."[178] This framework would likewise allow courts to properly scrutinize whether the use of other nascent technologies violate the Fourth Amendment.

VI. CONCLUSION

Real-time cellphone location tracking violates the Fourth Amendment under any regular circumstances as a trespass to an effect. The Framers specifically listed effects as protected under the Fourth Amendment and the public at the time understood this to mean personal property, like cellphones. Reading effects under its original meaning to include personal property would better accord search analysis with the Framers' enumerated protections. As reasoned in *Jones*, personal property rights are essential in the examination of whether the government's use of new technology infringes on privacy.

Technology advances exponentially and likewise so do law enforcement's tools to thwart crimes. Surveillance has a legitimate role to protect safety and national security interests. However, the government's indiscriminate, surreptitious, real-time monitoring of citizens threatens privacy protections fundamental to a functioning democracy

176. *Jones*, 565 U.S. at 418 (Alito, J., concurring).

177. *See* Brady, *supra* note 137, at 954–55 (citing Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 805 (2016) (discussing some of the conceptual difficulties associated with deciding whether digital data is an effect, and suggesting a virtual curtilage theory to protect data associated with personal property)).

178. Riley v. California, 573 U.S. 373, 392–93 (2014). The Court in *Riley* may have considered data to be paper or an effect. *See id.* at 393, 400 (comparing a cellphone to a "purse," "wallet," "camera[]," and "video player[]," and comparing data to "slip[s] of paper," "video tapes," "photo albums," and an "address book").

and "the role of the people as disciplinary observers of their government."[179] Such a vast surveillance state may create a chilling effect.[180]

Efforts at secrecy in the use of Stingrays and the murkiness in law around whether a warrant is required must be addressed with transparency and clarity. Applying existing doctrine leaves uncertainty about whether the use of a Stingray to gather location information constitutes a Fourth Amendment search.[181] In the face of that uncertainty, courts should look to the law of personal property embodied in the Original meaning of the Fourth Amendment's protection of effects.

179. David Gray, *Collective Rights and the Fourth Amendment After Carpenter,* 79 MD. L. REV. 66, 73 (2019). People may be afraid to voice opposition to government practices or otherwise feel constrained in their actions.

180. *Id.* Such a vast surveillance state could create a chilling effect where people will not voice opposition to government practices.

181. Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J. 943, 959 n.82 ("Anyone who has struggled to learn, teach, or apply *Katz*'s reasonable-expectation-of-privacy standard to the broad variety of real-world policing scenarios will appreciate why Fourth Amendment doctrine is so frequently characterized as 'a mess, an embarrassment, and a mass of contradictions.'") (quoting Kerr, *An Equilibrium Adjustment, supra* note 119, at 479).