Why Digital Policing Is Different

ANDREW GUTHRIE FERGUSON*

Many Fourth Amendment debates boil down to the following argument: if police can already do something in an analog world, why does it matter that new digital technology allows them to do it better, more efficiently, or faster? This Article addresses why digital is, in fact, different when it comes to police surveillance technologies. The Article argues that courts should think of these digital technologies not as enhancements of traditional analog policing practices but as something completely different, warranting a different Fourth Amendment approach. Properly understood, certain digital searches should be legally distinguishable from analog search precedent such that the older cases no longer control the analysis.

TABLE OF CONTENTS

I. INTRODUCTION

Many Fourth Amendment debates boil down to the following argument: if police can already do something in an analog world, why does it matter that new digital technology allows them to do it better, more efficiently, or faster? After all, if ten law enforcement agents can track your whereabouts for a month, what difference does it make if a GPS device tracks you for the same amount of time?[1]

*Professor of Law, American University Washington College of Law. Thank you to the editors and organizers of the *Ohio State Law Journal*'s Symposium: *The Right of the People to Be Secure: Modern Technology and the Fourth Amendment (2021)*. This Article was an invited contribution to this excellent symposium.

[1] Under existing law, short-term human surveillance in public spaces is allowed without a warrant. *See* United States v. Karo, 468 U.S. 705, 721 (1984). However, in *United States*

If a detective can stakeout your home for a year, what difference does it make if a digital pole camera watches the same home for a year?[2] If a police officer can surveil your backyard from a plane, what difference does it make if planes with wide-area digital cameras surveil all of the backyards of everyone in a city?[3] Of course, there are significant differences in terms of time, scale, and scope in the revealing nature of the police activity, but the open question is whether the new superpowers inherent in surveillance technology should change the Fourth Amendment analysis.[4] If, as scholars have suggested, "digital is different"[5] when it comes to technology-enhanced searches, the question is why.

This Article addresses why digital is, in fact, different when it comes to police surveillance technologies. The Article argues that courts should think of

---

v. Jones five members of the Supreme Court suggested that twenty-eight days of GPS (global positioning system) surveillance would require a warrant. *See* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in judgment); *id.* at 415 (Sotomayor, J., concurring) (agreeing with Justice Alito and the three other Justices joining his concurrence that long-term aggregated GPS tracking without a warrant violated the Fourth Amendment).

[2] Human stakeouts have long been a staple of policing. Hundreds of reported cases reference the term "stakeouts." *See, e.g.*, United States v. Nelson, 459 F.2d 884, 886 (6th Cir. 1972); *see also* William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1277 (1999) ("Stakeouts—observing the comings and goings of residents of and visitors to a private home, sometimes over a period of days—likewise require no Fourth Amendment justification."). However, the issue whether police can use a long-term pole camera has created a split in the courts. *Compare* United States v. Tuggle, 4 F.4th 505, 510–11 (7th Cir. 2021) (holding that a warrantless eighteen month pole-camera observation of a home was not a search for Fourth Amendment purposes), *cert. denied*, 142 S. Ct. 1107 (2022), *and* United States v. Houston, 813 F.3d 282, 285, 287–88 (6th Cir. 2016) (concluding that the government's use of pole cameras installed on public property and trained on the defendant's home for ten weeks did not constitute a Fourth Amendment search), *with* People v. Tafoya, 494 P.3d 613, 614 (Colo. 2021) ("[P]olice use of the pole camera to continuously video surveil Tafoya's fenced-in curtilage for three months, with the footage stored indefinitely for later review, constituted a warrantless search in violation of the Fourth Amendment.").

[3] The Supreme Court has allowed brief warrantless aerial overflight surveillance without a warrant. *See* California v. Ciraolo, 476 U.S. 207, 215 (1986). However, use of more sophisticated planes with wide-angle video capabilities has been found to be violative of the Fourth Amendment in at least one federal court. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333–36 (4th Cir. 2021) (en banc).

[4] The term "superpower" here references the superhuman capacity that certain technologies provide, for example, x-ray vision. *See* David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 1–3 (1996) (discussing the superpowers of new technologies).

[5] Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 951 (2016) ("So, while *Riley* perhaps left things unanswered that it could have addressed, it made very clear that when it comes to the Fourth Amendment, digital is different."); *see also* Jennifer Stisa Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUST SEC. (June 25, 2014), https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital [https://perma.cc/ 94RH-42EV].

these digital technologies not as enhancements of traditional analog policing practices but as something completely different, warranting a different Fourth Amendment approach. While superficially similar, in truth, everything from *the act* to *the result* to *the scalability of the technology* is different in the digital world and needs to be appreciated as such.[6] Properly understood, certain digital searches should be legally distinguishable from analog search precedent such that the older cases no longer control the analysis.

This Article advances one building block in the construction of a digitally-aware Fourth Amendment. It seeks to end reliance on the argument—since police could do something in an old-fashioned, analog world any digital equivalent is constitutional.[7] In other words, the Article seeks to explain why digital searches should be considered different and distinguishable in modern Fourth Amendment doctrine. This symposium contribution does not necessarily take on how that difference translates into a new Fourth Amendment search theory.[8] In earlier scholarship, I have attempted that theoretical task applying digital Fourth Amendment principles to facial recognition technology,[9] smart cities,[10] the "Internet of Things,"[11] and persistent surveillance systems.[12] Obviously, the Supreme Court has begun its own exploration in this space in *Riley v. California*[13] (smartphone data), *United States v. Jones*[14] (GPS data), and

---

[6] *See infra* Parts III.B.1, III.B.2.

[7] For example, in many of the pole camera cases that uphold police use of new surveillance technologies, courts rely on analogies to older, analog technologies. *See, e.g.*, *Tuggle*, 4 F.4th at 514–15 (citing approvingly to United States v. Knotts, 460 U.S. 276 (1983) (a beeper case) to argue that digital video cameras as mere enhancements did not violate a reasonable expectation of privacy), *cert. denied*, 142 S. Ct. 1107 (2022). Other examples will be discussed *infra*.

[8] The reason for framing the question as a "Fourth Amendment search theory" is that much of the modern Supreme Court's Fourth Amendment doctrine turns on the threshold question of whether there was a "search." As will be discussed, the Supreme Court has offered two "search" tests. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (defining a reasonable expectation of privacy test); United States v. Jones, 565 U.S. 400, 404–05 (2012) (defining a search test based on a physical intrusion with the intent to gather information).

[9] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1108 (2021) [hereinafter Ferguson, *Facial Recognition*].

[10] Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 49 (2020) [hereinafter Ferguson, *Sensor Surveillance*].

[11] Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 551 (2017) [hereinafter Ferguson, *Fourth Amendment*]; Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 808, 823 (2016) [hereinafter Ferguson, *Internet of Things*].

[12] *See generally* Andrew Guthrie Ferguson, *Persistent Surveillance*, ALA. L. REV. (forthcoming 2022) [hereinafter Ferguson, *Persistent Surveillance*], https://ssrn.com/abstract=4071189 [https://perma.cc/E9CJ-4GYH].

[13] Riley v. California, 573 U.S. 373, 403 (2014).

[14] United States v. Jones, 565 U.S. 400, 404 (2012).

Carpenter v. United States[15] (CSLI data)—the cases that gave rise to a "digital is different" framework.[16] This Article suggests those cases were correctly decided and hints at ways to further future-proof Fourth Amendment doctrine.[17]

This Article proceeds in two parts. In Part II, the Article explores the analog policing technologies that make up the corpus of surveillance cases in the Supreme Court, demonstrating why they serve as poor precedent for new digital surveillance technologies. In addition, this Part explores the Supreme Court's recent struggle to fit pieces of the analog puzzle into the world of digital surveillance. In Part III, the Article explores why digital policing is different in terms of what police are doing (the act), what police are receiving (the result), and how the technology can expand and evolve (the scalability). The goal of this analysis is to end—once and for all—blind reliance on analog precedent when it comes to digital policing questions.

II. THE ANALOG TECHNOLOGY ERA

The modern Fourth Amendment doctrine is anything but modern. In fact, it is built upon analogies to outdated technologies. The reality is that the constitutional principles expected to answer questions about city-wide camera systems,[18] self-driving smart cars,[19] and sensor-equipped drones,[20] among other digital surveillance innovations,[21] were created in response to a series of now antiquated technologies. This Part looks at the history of the Supreme Court's approach to technologically enhanced surveillance. Part II.A examines the pre-digital cases arising from policing technology in use in the 1960s, 1970s, and

---

[15] Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).

[16] Henderson, *supra* note 5, at 951; Granick, *supra* note 5.

[17] *See* Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018) [hereinafter Ferguson, *Future-Proofing*], https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment [https://perma.cc/MD79-G69G]; *Carpenter*, 138 S. Ct. at 2218 ("[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" (quoting Kyllo v. United States, 553 U.S. 27, 36 (2001))).

[18] *See* JOHN S. HOLLYWOOD, KENNETH N. MCKAY, DULANI WOODS & DENIS AGNIEL, RAND, REAL-TIME CRIME CENTERS IN CHICAGO: EVALUATION OF THE CHICAGO POLICE DEPARTMENT'S STRATEGIC DECISION SUPPORT CENTERS, at xi, 8–9 (2019) (detailing the extensive cameras system established in Chicago, Illinois); Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html [https://perma.cc/YC4Q-CZP7].

[19] Chris Vallance, *Self-Driving Car Stopped by San Francisco Police*, BBC (Apr. 12, 2022), https://www.bbc.com/news/technology-61080666 [https://perma.cc/74MA-YS68].

[20] Sidney Fussell, *Kentucky Is Turning to Drones to Fix Its Unsolved-Murder Crisis*, ATLANTIC (Nov. 6, 2018), https://www.theatlantic.com/technology/archive/2018/11/police-drone-shotspotter-kentucky-gun-911-ai/574723 [https://perma.cc/V9KT-LQJU].

[21] *See generally* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) [hereinafter FERGUSON, BIG DATA POLICING] (discussing the use of new policing technologies).

1980s. Part II.B examines the end of the analog era[22] as the Supreme Court has begun to recognize that digital technologies call for a different constitutional analysis.

A. *Pre-Digital Surveillance & the Fourth Amendment*

It is only a slight understatement to say that much of current Fourth Amendment theory turns on a response to a 1967-era cassette tape player equivalent.[23] The wire recorder technology at issue required two microphones to be physically taped to the top of a coin-operated phone booth in order to capture voices.[24] Such was the technology in *Katz v. United States* that gave rise to the "reasonable expectation of privacy" test and current Fourth Amendment doctrine.[25] The audio-cassette tape recording device was primitive compared to modern digital audio sensor capabilities.[26] It had to be manually affixed with tape atop a bank of pay phones.[27] FBI agents also had to manually turn the device on and off before and after each use.[28] In the *Katz* investigation, the

[22] The "analog era" is simply a term to denote the use of surveillance technologies largely dependent on human effort and not supported by sophisticated digital technology. *See* Woodrow Hartzog, Gregory Conti, John Nelson & Lisa A. Shay, *Inefficiently Automated Law Enforcement*, 2015 MICH. ST. L. REV. 1763, 1781.

[23] *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that a warrantless capturing of a telephone call with a tape recorder violated the Fourth Amendment); *see also* Brief for Petitioner at 5, *Katz*, 389 U.S. 347 (No. 35) ("Petitioner's conversation was overheard and recorded [and later transcribed] by means of a tape recorder which was placed on top of the middle booth. One of the three booths was placed out of order by the FBI with the consent of the telephone company." (citations omitted)).

[24] Brief for Respondent at 3, *Katz*, 389 U.S. 347 (No. 35) ("Connected to the recorder were two microphones, which were taped to the outside of two of the booths. None of the equipment (the recorder, the microphones and the fastenings) penetrated the booths." (footnote omitted) (citation omitted)).

[25] *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

[26] The technology behind audio-cassette recordings was only invented in 1962 and introduced to the United States in 1964. Katy Sommerfeld, *History of the Cassette Tape*, ANALOG, https://legacybox.com/blogs/analog/history-of-the-cassette-tape [https://perma.cc/ZBH8-BLWR].

[27] Brief for Petitioner, *supra* note 23, at 5 ("The recorder microphone was taped onto the booth and no part of the microphone physically penetrated the telephone booths." (citation omitted)).

[28] *Id.* at 5 ("The microphone was activated when Petitioner was a block away from the booth. The microphone was deactivated after Petitioner left the booth. Apparently, anybody could use the booth while the recording equipment was operative; in fact, on February 23, 1965, a stranger did use the booth and his conversation was recorded." (citations omitted)); Brief for Respondent, *supra* note 24, at 3–4 ("Each day, as petitioner approached a certain spot about a block and a half away from the telephones, agents in a radio car surveilling petitioner signaled other agents near the booths, who then attached and activated the recorder and microphones. After petitioner departed, the device was removed." (citation omitted)).

device was used for seven days,[29] and the recording device malfunctioned on one of the days.[30] The technology could record voices from the phonebooth in short segments but did not capture any other data.[31] As a standalone recording device, requiring physically present investigating officers,[32] and with limited storage capacity, the *Katz* technology provided a rather narrow collection opportunity with little concern about generalized, or over-broad police surveillance.[33] In holding that the warrantless application of the recording device violated the Fourth Amendment, Justice Harlan's concurrence reasoned that Charlie Katz had a subjective and objective reasonable expectation of privacy in his conversations such that police needed a warrant to intercept them.[34]

Early tracking devices were also similarly restricted in capacity. Unlike today's ubiquitous real-time locational services (available in phones and cars),[35] beeper tracking technology was limited by the near-field, limited spectrum broadcast range of then-existing radio transmissions.[36] Until the Court decided *Jones* and *Carpenter*,[37] Fourth Amendment rules around tracking in public turned on two beeper cases: *United States v. Knotts*[38] and *United States v. Karo*.[39] The tracking technology at issue in these cases involved a simple, battery-operated radio transmitter which emitted electronic signals that could be picked up by a

[29] Brief for Respondent, *supra* note 24, at 3 ("Every day from February 19 through February 25, 1965, F.B.I. agents placed a recording device on top of the bank of phone booths from which petitioner made his calls." (citation omitted)).

[30] Brief for Petitioner, *supra* note 23, at 5 ("On February 20, 1965, through February 25, 1965, inclusive, Petitioner was observed using the same phone booths and the agents of the FBI followed the same procedure of recording and transcribing his telephone conversations, although no tape recording was obtained on February 22, 1965, due to mechanical difficulties.").

[31] *See* Katz v. United States, 389 U.S. 347, 354 n.14 (1967).

[32] Brief for Respondent, *supra* note 24, at 3–4.

[33] *See Katz*, 389 U.S. at 354.

[34] *Id.* at 360–61 (Harlan, J., concurring).

[35] Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 408 (2013) ("Geolocation data can identify the location of wireless devices like cell phones. Although mobile phones are one popular source, geolocation data can also come from tablets, laptops, traditional desktops, and even cars.").

[36] *Tracking* Katz*: Beepers, Privacy, and the Fourth Amendment*, 86 YALE L.J. 1461, 1461 (1977) ("The beeper is a miniature, battery-powered radio transmitter that emits recurrent signals at a set frequency. By covertly attaching the beeper to a subject's property and monitoring its signals with a separate receiver, the police can electronically track the property, and often the subject, for distances of several miles and for as long as several weeks."); *see also* Richard H. McAdams, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 314–15 (1985) (discussing beeper technology and the Fourth Amendment in 1985 with analysis of the limits of the technology).

[37] United States v. Jones, 565 U.S. 400, 404 (2012); Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[38] United States v. Knotts, 460 U.S. 276, 285 (1983).

[39] United States v. Karo, 468 U.S. 705, 721 (1984).

hand-held radio receiver.[40] The radio transmitter had to be physically affixed to an object (a container) and required human police officers to physically possess the receiver as they tracked the transmissions.[41] The geographic range of the signals was limited, and the only information provided was the beeper's location.[42]

In *Knotts*, the Supreme Court held that the beeper-enhanced tracking was not a Fourth Amendment search because no information had been revealed that could not have been observed by officers trailing the beeper in public areas.[43] The Court analogized to visual surveillance that could (hypothetically) have been conducted on public roads and found that beepers merely "augment[] the sensory faculties bestowed upon" law enforcement.[44] In *Knotts*, the beeper signal led police to the area around a cabin where narcotics-making materials were seized.[45] Importantly for the Court, the beeper did not reveal any details from inside the cabin.[46]

In contrast, the Supreme Court in *Karo* held that a similar beeper investigation did violate the Fourth Amendment, but only because the beeper

---

[40] *Knotts*, 460 U.S. at 277 ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."); *Jones*, 565 U.S. at 429 n.10 (Alito, J., concurring in judgment) ("Even with a radio transmitter like those used in *United States v. Knotts* . . . or *United States v. Karo*, . . . such long-term surveillance would have been exceptionally demanding. The beepers used in those cases merely 'emit[ted] periodic signals that [could] be picked up by a radio receiver.' The signal had a limited range and could be lost if the police did not stay close enough." (quoting *Knotts*, 460 U.S. at 277)).

[41] *See Knotts*, 460 U.S. at 278; *Karo*, 468 U.S. at 708–09.

[42] The beeper only provided information about location, nothing more. *Knotts*, 460 U.S. at 284–85; *see also* David H. Goetz, Note, *Locating Location Privacy*, 26 BERKELEY TECH. L.J. 823, 839 (2011) ("[T]he beepers used in *Knotts* and *Karo* were simple radio transmitters of limited range that forced the agents tracking the device to stay in close physical proximity to the device.").

[43] *Knotts*, 460 U.S. at 281–82 ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); *see also id.* at 277 ("In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of respondent's codefendants. By monitoring the progress of a car carrying the chloroform Minnesota law enforcement agents were able to trace the can of chloroform from its place of purchase in Minneapolis, Minn[esota], to respondent's secluded cabin near Shell Lake, Wis[consin].").

[44] *Id.* at 282 ("Visual surveillance from public places along Petschen's route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation."); *see also id.* at 285 ("A police car following Petschen at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car.").

[45] *Id.* at 278–79.

[46] *Id.* at 285 ("But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

revealed the location of a bugged container inside a home.[47] The rationale for the different result turned on the argument that police could not have known the location of the container residing inside the house unless they had illegally entered the house.[48] Because police obtained constitutionally protected information without a warrant, this violated an expectation of privacy of things in a home.[49] The Court drew a distinction between public facing information and privately hidden information, protecting only the latter.[50]

In both cases, the beepers at issue revealed the location of an object.[51] The technology provided linear and relatively short-term tracking data about one container.[52] It was a single-use technology, directed at targets already under suspicion.[53] It also required human police officers to physically follow the device and thus gave the *Knotts* Court a plausible argument that the beeper did not reveal much more than the police could have seen with their own two eyes.[54] Compared to contemporary globally networked geolocational satellite systems and other geolocational tagging technologies that can reveal the location of millions of objects without police ever leaving their desks,[55] the beepers were simple radios limited in range and capabilities by their human controllers.

---

[47] United States v. Karo, 468 U.S. 705, 708, 714, 721 (1984) ("This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.").

[48] *Id.* at 715 ("The case is thus not like *Knotts*, for there the beeper told the authorities nothing about the interior of Knotts' cabin. The information obtained in *Knotts* was 'voluntarily conveyed to anyone who wanted to look . . . ,' here, as we have said, the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified." (quoting *Knotts*, 460 U.S. at 281)).

[49] *Id.* ("In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house.").

[50] *See id.* ("The monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant.").

[51] *Knotts*, 460 U.S. at 277; *Karo*, 468 U.S. at 708.

[52] In both cases the beeper was affixed to a container. *See* cases cited *supra* note 51.

[53] *See* cases cited *supra* note 51.

[54] *See Knotts*, 460 U.S. at 282. ("The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

[55] *See generally* UNIVERSAL SERV. ADMIN. CO., GEOLOCATION METHODS: A GUIDE TO SUCCESSFULLY COLLECTING BROADBAND DEPLOYMENT DATA, https://www.usac.org/wp-

In the same way it might seem strange that the Supreme Court's entire Fourth Amendment tracking/surveillance doctrine was built around old-school beepers, the Court's entire "third-party doctrine"[56] centered on similarly out-of-date technology—namely landline phone and paper bank records. For decades, *Smith v. Maryland*[57]—a case involving landline phones records from a phone company—along with *United States v. Miller*[58]—a case involving copies of paper bank records—controlled the analysis.[59] *Smith* is a technology case involving a pen register device that mechanically recorded outgoing phone numbers.[60] *Miller* is a non-technology case, involving the collection of paper bank documents (and microfilm copies of the records).[61] As technologies go, both have little in common with the massive global communications systems or fintech mobile banking options that now track everything we connect with or what we buy using digital technology.[62]

The technology at issue in *Smith v. Maryland* was a pen register.[63] At the time, pen registers were mechanical devices attached to a telephone line that transcribed dialed phone numbers on to a paper tape.[64] The technology converted "changes in electrical voltage caused by the turning of the telephone dial (or pressing of buttons on push button telephones)" into recognizable numbers.[65] Police requested that a telephone company place a pen register on Mr. Smith's landline to help prove that he was harassing a robbery victim.[66] The recorded numbers were used as evidence against him, and he raised a Fourth Amendment challenge that the numbers had been obtained without a warrant and in violation of his reasonable expectation of privacy.[67] In upholding the police action, the Supreme Court held that there is no expectation of privacy in the phone numbers conveyed

---

content/uploads/high-cost/documents/Tools/HUBBGeolocationMethods.pdf [https://perma.cc/GRJ2-4SB9] (discussing different geolocational technologies).

[56] *See generally* Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 829–30 (2022) (discussing the evolution of the third-party doctrine).

[57] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[58] United States v. Miller, 425 U.S. 435, 437 (1976).

[59] *Id.*; Jacobi & Stonecipher, *supra* note 56, at 834.

[60] *Smith*, 442 U.S. at 742–43 (discussing the pen register used to record phone numbers).

[61] *Miller*, 425 U.S. at 438 (describing the microfilm agents requested).

[62] *See generally* HILARY J. ALLEN, DRIVERLESS FINANCE: FINTECH'S IMPACT ON FINANCIAL STABILITY (2022) (discussing Fintech technology and the consequences of driverless finance).

[63] *Smith*, 442 U.S. at 737 (discussing the pen register at issue).

[64] Brief for Respondent at 2, *Smith*, 442 U.S. 735 (No. 78-5374) ("[A] pen register: 'is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line. It does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed.'" (quoting United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring and dissenting))).

[65] *Id.* at 3 (quoting United States v. N.Y. Telephone Co., 434 U.S. 159, 167 (1977)).

[66] *Smith*, 442 U.S. at 737.

[67] *Id.* at 737–38.

to a third-party phone company.[68] Police only obtained phone numbers that the user of the phone system knew were being recorded by the company for other purposes.[69] As such, there was no Fourth Amendment search and no need for a warrant.[70] Because the holding turned on the voluntary nature of information relinquished to third parties, this case became known for creating the "third-party doctrine" by which one loses an expectation of privacy if one turns over information to a third party that later turns it over to the government.[71]

Miller is an even stranger precedent for modern digital records. *Miller* only involved paper records and microfilm copies of those paper records.[72] *Miller* began with a prosecution of an individual who failed to pay taxes on illegally produced alcohol.[73] In order to prove the case, prosecutors subpoenaed two banks for financial records.[74] Agents physically went to the banks and personally examined paper copies and microfilm that detailed the defendant's financial circumstances.[75] The most technologically advanced event of the entire prosecution was the viewing of circa 1973 era microfilm.[76] The Supreme Court held that Miller had no reasonable expectation of privacy in documents he willingly shared with a third-party bank.[77] This case—and the third-party doctrine—has justified

---

[68] *Id.* at 742, 745–46 ("[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

[69] *See id.* at 742–43 ("Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls." (citation omitted)).

[70] *See id.* at 743–46.

[71] *Id.* at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."); *id.* at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[72] United States v. Miller, 425 U.S. 435, 438 (1976) ("At the Bank of Byron, an agent was shown microfilm records of the relevant account and provided with copies of one deposit slip and one or two checks. At the Citizens & Southern National Bank microfilm records also were shown to the agent, and he was given copies of the records of respondent's account during the applicable period. These included all checks, deposit slips, two financial statements, and three monthly statements.").

[73] *Id.* at 436.

[74] *Id.* at 437–38.

[75] *Id.* at 438.

[76] *See id.*

[77] *Id.* at 442 ("Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena,

police access to a host of digital evidence from all sorts of third-party providers from cellphones to smart technology.[78]

Oddly, one of the most protective Fourth Amendment cases involved a technology that merely recorded heat signals. *Kyllo v. United States* centered on the use of a rather unsophisticated thermal imaging device to identify elevated heat levels originating from a home.[79] In *Kyllo*, police suspected that Danny Kyllo was using indoor grow lights to cultivate marijuana.[80] To confirm these suspicions, police investigators used an Agema Thermovision 210 thermal imager to convert the heat patterns into visible images.[81] Those images showed a suspiciously high heat output in certain rooms which was used to justify a search warrant into Kyllo's home looking for marijuana.[82]

---

we perceive no legitimate 'expectation of privacy' in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

[78] *See* Jacobi & Stonecipher, *supra* note 56, at 825–26, 838–39.

[79] Kyllo v. United States, 533 U.S. 27, 29 (2001) ("In order to determine whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex.").

[80] *Id.* at 29.

[81] *Id.* at 29–30 ("Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images.").

[82] Brief for Respondent at 4, *Kyllo*, 533 U.S. 27 (No. 99-8508) ("On January 16, 1992, between 3:30 and 4:00 a.m., Oregon National Guard Sergeant Dan Haas used an Agema 210 thermal imager to scan the triplex where Tova Shook and petitioner lived. The thermal scan showed a high amount of heat emanating from the roof over the garage and the side wall of petitioner's house. In addition, it showed that petitioner's house was emitting more heat than the other houses in the triplex. The unusual heat loss detected by the imager was consistent with the heat loss associated with marijuana grow operations that Detective Haas had observed in the past." (citations omitted)).

The thermal technology at issue only registered heat signatures.[83] As a handheld device, it needed human presence to capture the information.[84] In addition, the device could only scan a narrow range of structures (here a triplex which included Kyllo's home).[85] The revealed information simply included levels of heat radiating off the house.[86] No details about people, activities, or other information could be identified from this version of the thermal imaging device.[87] While the Supreme Court acknowledged a real concern with more invasive, future technologies, this particular device was not revealing of anything but comparative radiation (heat) levels among a few houses.[88] Yet, the Supreme

[83] *Id.* at 6 ("A thermal imager is able to detect infrared radiation. The imager gathers the infrared radiation that is emitted from the outside surface of the object at which it is pointed. The imager then converts what it has detected into a visible image that it displays on a screen. An imager is passive; it does not send out any rays. It is similar to a camera in that respect, except that a camera collects energy from the visible range of the electromagnetic spectrum, while imagers collect information from the infrared range. When the Agema 210 imager detects areas that are relatively warm, it displays them as white; when it detects areas that are relatively cool, it displays them as black; and when it detects areas between the extremes, it displays them as shades of gray. A polarity invert button on the imager changes the warmer spots from white to black and the cooler spots from black to white. The Agema 210 imager shows only relative heat patterns; it does not measure temperature in absolute terms." (citations omitted)).

[84] *See id.* at 8 ("Detective Haas performed the thermal scan at issue in this case from the passenger seat of Agent Elliott's vehicle across the street from the front of petitioner's house. He then drove across the street and viewed the building from the back of the house. A videotape recording of the thermal scan of petitioner's house shows that the exterior of the center building (petitioner's house) is radiating more heat than the exterior of the other two buildings." (citations omitted)).

[85] *See id*. at 8.

[86] *Id.* at 26 ("The district court found that the imager 'shows a crude visual image of the *heat* being radiated from the *outside* of the house,' and that '[t]he device cannot and did not show any people or activity within the walls of the structure.'" (citation omitted)).

[87] *See* Brief for Respondent at 7, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508) ("When a thermal imager is pointed at a wall composed of normal construction materials, such as lath, plaster, plasterboard, stucco, or brick, it detects the radiation that is emitted or reflected from the outside surface of the wall. An imager cannot see through a wall. In an in-court demonstration, a thermal imager was pointed at a window, and it could not detect the person standing behind it. In certain circumstances, however, a thermal imager has the capacity to detect radiant heat through windows. Whether it could do so would depend on the type of glass, the thickness of the glass, the wavelength of the camera, and the kind of lens that is used. A thermal imager cannot 'see' an object through thin curtains unless the object is directly pressed up against the curtains. An imager can detect activity through an open window." (citations omitted)).

[88] Kyllo v. United States, 533 U.S. 27, 30, 35–36 (2001) ("The scan of Kyllo's home took only a few minutes and was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex.").

Court found the use of the technology a Fourth Amendment search because the intrusion violated a reasonable expectation of privacy.[89]

The final category of policing technologies involves aerial surveillance. In *California v. Ciraolo*, police used a private airplane to fly over a suspect's home to observe illegal marijuana growing on his property.[90] In *Florida v. Riley*, police used a helicopter to view "with [the officer's] naked eye" illegal marijuana growing near the home.[91] In both cases, the Supreme Court emphasized the non-technologically enhanced human vision of the officers as key to the search question.[92] Thus, while air transport technology was utilized (i.e., the plane/helicopter), the Supreme Court emphasized that these were not to be considered technology-enhanced surveillance cases, but only cases involving human eyesight.[93] In fact, even though a camera was used in *Ciraolo*, the Supreme Court explicitly clarified

---

[89] *Id.* at 34, 40 ("To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' . . . constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

[90] California v. Ciraolo, 476 U.S. 207, 209 (1986) ("Officer Shutz, who was assigned to investigate, secured a private plane and flew over respondent's house at an altitude of 1,000 feet, within navigable airspace; he was accompanied by Officer Rodriguez. Both officers were trained in marijuana identification. From the overflight, the officers readily identified marijuana plants 8 feet to 10 feet in height growing in a 15- by 25-foot plot in respondent's yard.").

[91] Florida v. Riley, 488 U.S. 445, 448 (1989) ("When an investigating officer discovered that he could not see the contents of the greenhouse from the road, he circled twice over respondent's property in a helicopter at the height of 400 feet. With his naked eye, he was able to see through the openings in the roof and one or more of the open sides of the greenhouse and to identify what he thought was marijuana growing in the structure.").

[92] *Ciraolo*, 476 U.S. at 214 (describing the police actions as "simple visual observations from a public place"); *Riley*, 488 U.S. at 450 ("The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye." (quoting *Ciraolo*, 476 U.S. at 215)).

[93] *Ciraolo*, 476 U.S. at 213 ("The observations by Officers Shutz and Rodriguez in this case took place within public navigable airspace, see 49 U.S.C. App. § 1304, in a physically nonintrusive manner; from this point they were able to observe plants readily discernible to the naked eye as marijuana. That the observation from aircraft was directed at identifying the plants and the officers were trained to recognize marijuana is irrelevant."); *Riley*, 448 U.S. at 449–50.

that it was only addressing the human observation (not the use of the camera technology).[94] The same human-centered argument was followed in *Riley*.[95]

Analyzed carefully, *Ciraolo* and *Riley* are not really technology cases at all. While slightly disingenuous to say that man-made flight is not a technological enhancement, the Court focused on unenhanced human eyesight to determine the scope of Fourth Amendment protections.[96] These cases, thus have little to say about aerial surveillance that requires non-human observation or technological enhancements beyond ordinary sight.[97]

The aerial overflight cases do include one technologically-enhanced exception. *Dow Chemical Co. v. United States* involved an environmental investigation into a large commercial industrial complex.[98] At issue was an aerial mapping camera that could fly as high as 12,000 feet and take detailed images of the ground-level complex.[99] The EPA used the mapmaking photographs to capture images of the external structures of the Dow Chemical complex.[100] Although the technology

---

[94] *Ciraolo*, 476 U.S. at 212 n.1 ("Because the parties framed the issue in the California courts below and in this Court as concerning only the reasonableness of aerial observation generally . . . without raising any distinct issue as to the photograph attached as an exhibit to the affidavit in support of the search warrant, our analysis is similarly circumscribed. It was the officer's observation, not the photograph, that supported the warrant. Officer Shutz testified that the photograph did not identify the marijuana as such because it failed to reveal a 'true representation' of the color of the plants: 'you have to see it with the naked eye.'" (citations omitted)); *see also* Brief for Petitioner at 8–9, *Ciraolo*, 476 U.S. 207 (No. 84-1513) ("Without visual aids, Detective Schutz [sic] and Agent Rodriguez identified, by its highlighted green color, a 15 by 25 foot marijuana garden of 8 to 10 foot tall plants in the backyard of 2085 Clark Avenue. The officers photographed the garden using a thirty-five millimeter camera.").

[95] Brief for Petitioner at 7–8, *Riley*, 488 U.S. 445 (No. 87-764) ("The deputy and a pilot employed by the Pasco County Sheriff's Office approached the property by helicopter at an altitude of approximately 400 feet. As the helicopter approached the property, Deputy Gell, using a camera with a telephoto lens, took photographs of the mobile home and greenhouse. The evidence is unclear as to whether the helicopter descended below 400 feet, but it did circle over the greenhouse twice while the deputy observed the property. Deputy Gell testified that through the openings in the roof and through one or more of the open sides of the greenhouse, he could see and identify growing marijuana plants."); *see also id.* at 10 ("In other words, although the deputy took two aerial photographs using a camera with a telephoto lens, he could see these 6-12 foot plants with his naked eye.").

[96] *Riley*, 488 U.S. at 450; *Ciraolo*, 476 U.S. at 215.

[97] Marc Jonathan Blitz, James Grimsley, Stephen E. Henderson & Joseph Thai, *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49, 65–77 (2015) (discussing the aerial surveillance doctrine of the Supreme Court).

[98] Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).

[99] *Id.* at 229 ("EPA employed a commercial aerial photographer, using a standard floor-mounted, precision aerial mapping camera, to take photographs of the facility from altitudes of 12,000, 3,000, and 1,200 feet. At all times the aircraft was lawfully within navigable airspace.").

[100] *Id.* at 238.

could not see inside the buildings,[101] the sophisticated and expensive camera did provide images well beyond the capacity of any human, and did potentially raise Fourth Amendment concerns about the privacy of the commercial enterprise.[102] Nevertheless, the Supreme Court upheld the warrantless use of this technology, emphasizing the industrial nature of the operation, which the Court distinguished from actions around private homes.[103]

It is hard to know what to make of *Dow Chemical*. The Court clearly emphasized a distinction between private homes and industrial property.[104] The case was also decided the same day as *Ciraolo*, which focused on what human senses could observe.[105] Yet, the government cameras at issue were very powerful and potentially could impact privacy in a host of other areas.[106] While the Court acknowledged the concern about revealing intimate associations, objects, and activities, it still allowed the government surveillance.[107] It is an open question whether *Dow Chemical* has application to ordinary police investigations (not involving commercial environmental enforcement).[108]

In summary, with the exception of *Dow Chemical*, the canon of seminal Fourth Amendment search cases focused on old fashioned, non-digital

---

[101] *Id.* ("Here, EPA was not employing some unique sensory device that, for example, could penetrate the walls of buildings and record conversations in Dow's plants, offices, or laboratories, but rather a conventional, albeit precise, commercial camera commonly used in mapmaking.").

[102] *See id.* ("It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant. But the photographs here are not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give EPA more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment. The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems.").

[103] *Id.* at 238–39. The Supreme Court tried to make this private home/commercial property distinction clear in *Kyllo v. United States*, 533 U.S. 27, 33 (2001) ("While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical*, we noted that we found 'it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened.'" (quoting *Dow Chem. Co.*, 476 U.S. at 237 n.4)).

[104] *Dow Chem. Co.*, 476 U.S. at 238 ("[U]nlike a homeowner's interest in his dwelling, '[t]he interest of the owner of commercial property is not one in being free from any inspections.'" (quoting Donovan v. Dewey, 452 U.S. 594, 599 (1981))).

[105] *Id.* at 227; California v. Ciraolo, 476 U.S. 207, 207 (1986).

[106] *See Dow Chem. Co.*, 476 U.S. at 229.

[107] *Ciraolo*, 476 U.S. at 215 n.3 (1986) ("In *Dow Chemical Co. v. United States* . . . decided today, we hold that the use of an aerial mapping camera to photograph an industrial manufacturing complex from navigable airspace similarly does not require a warrant under the Fourth Amendment. The State acknowledges that '[a]erial observation of curtilage may become invasive, either due to physical intrusiveness or through modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.' Brief for Petitioner 14–15.").

[108] *See Dow Chem. Co.*, 476 U.S. at 239.

technologies that collected a limited amount of information. The scale, scope, and capacity of these technologies largely mirrored the human capabilities of police officers without any technology. The technologies tended to be one-off uses, requiring physically present, governmental actors, and did not create digital systems of ongoing surveillance capabilities. The technologies are also decidedly out of date—symbolizing the limits of existing innovation in the 1970s, 1980s, and 1990s.

Each one of these limits is important to understand because they still shape the "reasonable expectation of privacy" doctrine in the twenty-first century. First, analog surveillance essentially mirrored human surveillance capabilities. Second, analog surveillance tended to be single, discrete acts of observation, not continuous collection. Finally, the technological tool being used provided only a limited amount of information about a limited number of people, and was not a system of widespread or ever-expanding, enhanced surveillance.

B. *Emerging "Digital Is Different" Cases*

The early Fourth Amendment cases still control analysis,[109] although they have been augmented by three Supreme Court cases which more directly address whether "digital is different" when it comes to new technologies.[110] These cases will be briefly discussed in an effort to demonstrate that while a digital Fourth Amendment has yet to materialize in any coherent manner, efforts have been made to acknowledge the need for a new approach.[111]

In chronological order, first, the Supreme Court held that police needed a warrant to search a smartphone even incident to arrest.[112] At issue in *Riley v. California* was a warrantless search of photos in a smartphone after an arrest.[113] The Court distinguished analog precedent that had generally allowed automatic warrantless searches of arrestees' property under the search incident to arrest

[109] For example, the District Court in the *Leaders of a Beautiful Struggle* applied the traditional aerial overflight cases in a pretty straightforward way, even though the Persistent Surveillance Systems planes were far more sophisticated than in *Ciraolo* or *Riley* and involved more than a naked eye observation. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 702, 704–05, 712–14 (D. Md.) (2020), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

[110] *See generally* United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).

[111] Interestingly, only one of the three cases involves direct use of police-operated surveillance technology (*Jones*, 565 U.S. at 403—GPS tracking technology), as opposed to law enforcement accessing already existing consumer-generated data (*Riley*, 573 U.S. at 385—smartphones) (*Carpenter*, 138 S. Ct. at 2208—CSLI data).

[112] *Riley*, 573 U.S. at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

[113] Police believed that photographs connecting Riley to criminal activity would be discovered in his smartphone. *Id.* at 379.

exception.[114] Focusing on the qualitatively and quantitatively different nature of digital information stored on a smartphone, the Court recognized that the smartphone data was a far greater privacy risk than any physical object previously allowed to be searched incident to arrest.[115] The Court's holding acknowledged that simplistic analogies to non-digital precedent (involving physical objects like wallets, etc.) no longer made sense in a digital age.[116]

Riley is well acknowledged to be the first Supreme Court case really to examine why digital is different when it comes to personal data.[117] The amount of information stored on a smartphone (involving communications, financial records, photographs, calendars, and contacts to name a few) is exponentially more revealing than anything that might have been carried on a person before.[118] In fact, smartphones may well hold more private information than homes these days, as they are the single source of most of our digital communications, papers, and contacts with the world.[119] Finally, the smartphone data at issue was not just limited to the smartphone itself, as the data could be stored on the device and/or the cloud in equal measure.[120] Giving police warrantless access to some data might open the door to other private data connected to the smartphone device.

---

[114] *See id.* at 400 ("[T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery.").

[115] *Id.* at 393–94 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[116] *See id.* at 393–94 ("[A] cell phone's capacity allows even just one type of information to convey far more than previously possible.").

[117] Michael Mestitz, Note, *Unpacking Digital Containers: Extending* Riley*'s Reasoning to Digital Files and Subfolders*, 69 STAN. L. REV. 321, 323–24 (2017) ("*Riley* in particular represents the Court's unanimous acknowledgement that digital containers are, at least in some respects, different in kind from their physical counterparts.").

[118] *Riley*, 573 U.S. at 394–95 ("The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." (footnote omitted)).

[119] *Id.* at 396–97 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A 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—unless the phone is.").

[120] *See id.* at 397 (discussing cloud computing and storage).

The Supreme Court recognized that blind reliance on precedent just no longer made sense in the interconnected digital age, and required a warrant to search the smartphone data.[121]

The Supreme Court followed *Riley* with *Jones v. United States*, a case that involved the use of long-term GPS surveillance tracking of a suspected drug dealer.[122] The majority in *Jones* decided the case on a trespass theory, finding the physical intrusion of placing the GPS device on a vehicle constituted a search for Fourth Amendment purposes.[123] Five Justices, however, concurred in judgment finding that long-term warrantless tracking of a vehicle violated a reasonable expectation of privacy under *Katz* and thus the Fourth Amendment.[124] As Justice Sotomayor reasoned, the long-term tracking revealed too many of the "privacies of life" that threatened political, religious, associational, and other personal freedoms.[125] The majority distinguished the rudimentary beeper technology cases (*Knotts/Karo*) from the more sophisticated GPS technology deployed in *Jones*.[126] Not only was the technology more precise and revealing, but because of the way GPS technology worked, no human agent was needed to follow the car, thus expanding the capacity of police to track more people.[127] These capabilities to track Mr. Jones or anyone (or everyone) without a warrant raised a privacy and security concern that several Supreme Court Justices could not countenance.[128]

---

[121] *Id.* at 386 ("But while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones."); *see also id.* at 386 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [prior precedent].").

[122] United States v. Jones, 565 U.S. 400, 402–03 (2012).

[123] *Id.* at 404–05 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

[124] *See id.* at 415–16 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); *id*. at 427, 430 (Alito, J., concurring in judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

[125] *Id.* at 415–16 (Sotomayor, J., concurring) ("I agree with JUSTICE ALITO that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" (quoting *id.* at 430 (Alito, J., concurring in judgment))).

[126] *Id.* at 408–10 (discussing United States v. Knotts, 460 U.S. 276 (1983) and United States v. Karo, 468 U.S. 705 (1984)).

[127] *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment); *see also* United States v. Houston, 813 F.3d 282, 286, 287–88 (6th Cir. 2016) (discussing the use of surveillance via pole cameras).

[128] *Jones*, 565 U.S. at 403 n.1, 404; *id.* at 429–31 (Alito, J., concurring in judgment).

Again, like in *Riley*, the Court acknowledged that digital surveillance was different for Fourth Amendment considerations which necessitated a cabining of analog precedent.[129]

The insight about digital privacy voiced by the concurring Justices in *Jones* was adopted by the majority in the Supreme Court's most significant digital surveillance case, *Carpenter v. United States*.[130] *Carpenter* involved the acquisition of cell-site location information ("CSLI") records of a man suspected of being involved in a series of Radio Shack robberies.[131] Records of the suspect's cell site location were obtained by police without a warrant, and were challenged as a Fourth Amendment violation.[132] The Supreme Court in *Carpenter* held that the acquisition of this information without a warrant violated a reasonable expectation of privacy.[133] Again, the reasoning turned on the aggregating, retrospective, permeating, and revealing nature of the data captured.[134] This reality of the type of information at issue distinguished cell site location records from other third-party records cases (i.e., *Smith/Miller*).[135] *Carpenter* is groundbreaking for many reasons, but one is that it adopts the idea that warrantless acquisition of third-party digital information can create a cognizable Fourth Amendment harm.[136]

The technology at issue in *Carpenter* is not comparable with earlier pre-digital police surveillance cases. As the Supreme Court recognized, the nationwide cell site network allowed police to obtain location data on almost any person

---

[129] *See Jones*, 565 U.S., at 429 (Alito, J. concurring in judgment) ("In the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." (footnote omitted)).

[130] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.").

[131] *Id.* at 2212, 2216 ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.").

[132] *Id.* at 2212.

[133] *Id.* at 2221 ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

[134] *Id.* at 2219–20 ("[M]echanically applying the third-party doctrine to this case . . . fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

[135] *Id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.").

[136] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019).

with a cell phone.[137] Because of the way cell phones work—connected to cell towers—the tracking was inescapable.[138] Because of ubiquitous phone use, the tracking was basically automatic and involuntary.[139] And, because of the systems in place to log calls, the network created a vast trove of digital clues that could be mined for insights all without agents doing anything but issuing a subpoena for the information.[140]

For purposes of this Article, four related points are notable from these three recent cases. First, the Supreme Court implicitly acknowledged that "digital is different" even if it was not clear how courts should interpret the Fourth Amendment in the digital age.[141] Second, this insight opens the door to argue that analog precedent may no longer control analysis of new forms of digital surveillance. To be clear, the Court did not reject analog precedent, but nor did the Court rely on these cases to answer new surveillance questions.[142] Third, the Fourth Amendment was interpreted to protect both direct police surveillance (like the GPS device in *Jones*) and law enforcement acquisition of indirect surveillance data (like the CSLI records in *Carpenter*). Fourth, the Court recognized the changing nature of surveillance brought on by new technology. While not agreeing on how the Fourth Amendment should adapt to new surveillance threats, the Court acknowledged the shifting landscape.[143] These insights help distinguish traditional Fourth Amendment cases from the new technological challenges that will redefine policing and Fourth Amendment liberties in the future.

III. DIGITAL POLICING

In contrast to the antiquated policing technologies of early Fourth Amendment cases, and even compared to the more modern technologies of GPS, CSLI, and smartphone/cloud storage discussed in Part II.B, today's police have new digital surveillance systems at their disposal. As I and others have

---

[137] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("[B]ecause location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

[138] *See* Matthew Tokson, *Inescapable Surveillance*, 106 CORNELL L. REV. 409, 418–19 (2021).

[139] *Carpenter*, 138 S. Ct. at 2218; *see* Ohm, *supra* note 136, at 376–78 (discussing how inescapable and automatic forms of data collection is a Fourth Amendment concern).

[140] *See id.* at 2218–19 ("Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years.").

[141] *See id.* at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

[142] *Id.* at 2220 ("Our decision today is a narrow one.").

[143] *Id.* at 2219–20.

written about previously, the types of new policing technologies have rapidly expanded, far exceeding their first generation, analog predecessors.[144] While a full accounting of big data policing technologies is beyond the scope of this Article, the following brief summary gives a vision of the digital surveillance tools available to police.

A. *Digital Policing Technologies*

Police surveillance technologies are best thought of as a series of concentric circles with overlapping capabilities focused on the targets of criminal prosecution. From the outer circles of pure monitoring capabilities, to inner rings of investigation through indirect acquisition of consumer data or direct digital surveillance, to the evidentiary use of forensic data in trial, the technologies look like a bulls-eye with criminal suspects in the center.

In the outer circle, policing technologies generate new monitoring capabilities.[145] These technologies offer police the ability to observe patterns of criminal (and non-criminal) activities in new ways.[146] As surveillance monitoring systems, these technologies may not end up as trial evidence, but are always on—watching.[147] For example, in Chicago, Illinois, the Chicago Police Department has created local "real-time crime centers" to monitor city streets.[148] Approximately 30,000 video cameras are linked together with additional crime data to watch the streets in real time.[149] Police can sit in their district command centers and monitor criminal incidents.[150] Police in Hartford, Connecticut operate a video analytics program called BriefCam to search city surveillance cameras for particular objects

---

144 *See generally* FERGUSON, BIG DATA POLICING, *supra* note 21.

145 The term "monitoring" denotes the observational capacities of the technologies. *See generally* Barry Friedman & Elizabeth G. Jánszky, *Policing's Information Problem*, 99 TEX. L. REV. 1, 17–24 (2020) (discussing monitoring technologies). Monitoring technologies may not be used as evidence in criminal cases. In fact, monitoring technologies may not even be reviewed by police (for example, stored footage in CCTV cameras). Instead, these technologies exist to watch areas or people without any specific investigative goal or purpose. Monitoring technologies, of course, can be used in prosecutions, but need not be so used. Examples of monitoring technologies include automated license plate readers, surveillance cameras, gunshot detection systems, and automated social media scanning software. Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205, 209, 225, 258, 276 (2021).

146 FERGUSON, BIG DATA POLICING, *supra* note 21, at 2–3.

147 *See id.*

148 Williams, *supra* note 18.

149 *Id.*; *see* HOLLYWOOD, MCKAY, WOODS & AGNIEL, *supra* note 18, at xi.

150 HOLLYWOOD, MCKAY, WOODS & AGNIEL, *supra* note 18, at xi; *Chicago Police Launch Their Latest 'Nerve Center' in Bid to Fight Crime with High-Tech Tools*, CBSNEWS (June 25, 2020), https://chicago.cbslocal.com/2020/06/25/chicago-police-launch-their-latest-nerve-center-in-bid-to-fight-crime-with-high-tech-tools/ [https://perma.cc/WV9U-8A4M].

or activities.[151] Sophisticated object recognition analytics technology allows police to find particular cars or really any identifiable object in the video with a quick search of the existing data.[152] In Los Angeles, data analytics in the form of Palantir's Gotham program allows police to monitor criminal patterns and connect groups of individuals.[153] The social network analysis system allows individuals and groups to be linked together to identify relationships and connections.[154] Other cities use predictive policing systems to guide police patrols.[155] In these jurisdictions, past crime data is fed into an algorithm to shape patrol patterns and target particular areas of a city.[156] A growing number of cities have incorporated ever-present cameras, police-worn body cameras, ShotSpotter gunshot detectors, and automated license plate readers ("ALPRs") into their ordinary monitoring of incidents and activities.[157] These technologies allow police to collect data on arrests, gunshots, and stolen cars in a particular geographic area.[158]

Each of these surveillance systems operates independent of any particular police investigation, collecting information widely, broadly, and indiscriminately. The vast majority of the data collected is never used for criminal prosecution,

---

[151] Eoin Higgins, *Pre-Crime Policing is Closer Than You Think, and It's Freaking People Out*, VICE (June 12, 2018), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-many-cameras-precrime [https://perma.cc/9CC6-G24G].

[152] JAY STANLEY, ACLU, THE DAWN OF ROBOT SURVEILLANCE: AI, VIDEO ANALYTICS, AND PRIVACY 17–19 (2019), https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf [https://perma.cc/QY5C-AARD] (discussing video analytics).

[153] Mark Harris, *How Peter Thiel's Secretive Data Company Pushed into Policing*, WIRED (Aug. 9, 2017), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing [https://perma.cc/YS2T-47AS]; *see* Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOC. REV. 977, 983, 987 (2017) [hereinafter Brayne, *Big Data Surveillance*].

[154] Brayne, *Big Data Surveillance*, *supra* note 153, at 992; *see* SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING 54 (2021) (detailing the role of social network analysis in LAPD's investigative systems).

[155] Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1180 (2017).

[156] Ellen Huet, *Server and Protect: Predictive Policing Firm PredPol Promises to Map Crime Before It Happen*s, FORBES (Feb. 11, 2015), http://www.forbes.com/sites/ellenhuet/2015/02/11/predpol-predictive-policing/#175113db407f [https://perma.cc/4BTQ-6W52]. *But see* Avi Asher-Schapiro, *California City Bans Predictive Policing in U.S. First*, REUTERS (June 24, 2020), https://www.reuters.com/article/us-usa-police-tech-trfn/california-city-bans-predictive-policing-in-u-s-first-idUSKBN23V2XC [https://perma.cc/GD4C-4J8H].

[157] *See, e.g.*, Friedman & Jánszky, *supra* note 145, at 18, 49 (discussing body cameras and ALPR technology). Erica Goode, *Shots Fired, Pinpointed and Argued Over*, N.Y. TIMES (May 28, 2012), www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html [https://perma.cc/3X49-NUZU]. *See generally* Ferguson, *Sensor Surveillance*, *supra* note 10, at 52 (2020).

[158] Friedman, *supra* note 145, at 18; Goode, *supra* note 157.

however, the data could be used if needed.[159] Thus, for example, if a video from a networked camera captured a criminal act, then that footage could be used as evidence in a later criminal prosecution.[160] Monitoring technologies turn into prosecution evidence because—on occasion—the continuous monitoring captures the crime.[161]

Moving inwards within our concentric circles are more targeted police investigations. Police now have access to indirect consumer data sources available through subpoenas or warrants.[162] In a digital world, individuals create a lot of incriminating evidence.[163] For example, smart cars reveal driving patterns, location, and occasionally videotape a hit and run.[164] Smart homes reveal personal preferences, habits, and digital assistants have been used to investigate serious criminal offenses occurring in the home.[165] Internet of Things-enabled home video

---

[159] Almost all "monitoring" technologies are dual use and can be used in prosecution. If the always-on persistent surveillance monitoring technologies is searchable, it will be the source of incriminating information useful for prosecutions. *See* Ferguson, *Persistent Surveillance*, *supra* note 12, at 7.

[160] *See* BARRY FRIEDMAN, FARHANG HEYDARI, EMMANUEL MAULEÓN & MAX ISAACS, POLICING PROJECT, CIVIL RIGHTS AND CIVIL LIBERTIES AUDIT OF BALTIMORE'S AERIAL INVESTIGATION RESEARCH (AIR) PROGRAM 14, 17–18 (Nov. 2020) [hereinafter, POLICING PROJECT] ("The most useful of these ground technologies is BPD's high-definition cameras, known as 'CitiWatch cameras.' Each of these cameras has a field of view spanning nearly two city blocks. The video resolution of these cameras is high enough to, on occasion, show a vehicle's license plate number, make, and model, or the face, clothing, or other identifying characteristics of an individual in the vehicle. PSS has direct access to CitiWatch footage—in one sample investigation we reviewed, one tracked subject passed by over 70 cameras as they moved through Baltimore—though they do not have the ability to pan or zoom in. PSS analysts select and share still images from these cameras with detectives.").

[161] *See id.* at 17–18.

[162] *Id.* at 26.

[163] *See, e.g.*, Ferguson, *Internet of Things*, *supra* note 11, at 813–15, 819–20 (cataloging the rise of digital tracking sensor devices).

[164] Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L. REV. 141, 199–200 (2020) ("Connected cars can also be very invasive. While yesterday's drivers could reasonably think of their in-car time as a private moment, today's BMWs come with Alexa built-in, and perhaps listening in as well. Other cars may soon have sensors capable of voice or facial recognition of all passengers, allowing tailoring of the driving experience to their preferences and health monitoring of drivers, but also collection of yet more information about the car's use."); Geoffrey Fowler, *My Car Was in a Hit-and-Run. Then I Learned It Recorded the Whole Thing*, WASH. POST (Feb. 27, 2020), https://www.washingtonpost.com/technology/2020/02/27/tesla-sentry-mode/ [https://perma.cc/7YER-L7UF] (describing the eight cameras on his Tesla car).

[165] *See* James O'Toole, *Cops Can Access Your Connected Home Data*, CNN (June 16, 2014), https://money.cnn.com/2014/06/16/technology/smart-home-footage/index.html [https://perma.cc/TJ3G-9KPS]; Meagan Flynn, *Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over*, WASH. POST (Nov. 14, 2018), https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/?Noredirect=on&utm_term=.250732055355 [https://perma.cc/THW3-KRB2]; Elliott C. McLaughlin &

systems capture both burglars and inter-family abuse.[166] Smartphones reveal our private lives connected to the cloud, and social media all of the activities we want to share with others.[167] Almost all digital technology reveals time, place, and allows inferences of activities, making it helpful for police investigators trying to piece together what happened at a particular time or to monitor suspects involved in possible ongoing criminal acts.[168] With the appropriate legal process (subpoena/warrant), prosecutors can access all of these digital clues by simply requesting the evidence from the private technology provider or platform.[169]

Overlapping these indirect police investigation technologies are more direct methods of police surveillance. In many cases police have a suspect and are using sophisticated technologies to investigate activities and generate evidence. For example, police can track individuals by affixing GPS technologies on moving objects (vehicles, luggage),[170] can identify a cell phone anywhere it is located using Stingray devices,[171] or can identify all the electronic devices in a specific area with a Geofence warrant.[172] Long-term pole cameras might watch a home for eighteen months at a time.[173] Facial recognition and biometric

---

Keith Allen, *Alexa, Can You Help with This Murder Case?*, CNN (Dec. 28, 2016), http://edition.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html [https://perma.cc/ES7D-WLBW].

[166] *See* Caroline Haskins, *New Map Reveals That At Least 231 Cities Have Partnered with Ring*, VICE (Aug. 8, 2019), https://www.vice.com/en_us/article/qvg4vx/new-map-reveals-that-at-least-231-cities-have-partnered-with-ring [https://perma.cc/8X6Q-HAS2]; *see also* Tabetha Soberdash, *Domestic Violence in the Era of the Smart Home: Using Smart Home Technology Evidence to Help Victims of Abuse*, 27 RICH. J.L. & TECH. 1, 3–5 (2020) (discussing inter-family cases).

[167] *See* Riley v. California, 573 U.S. 373, 397–88 (2014); Rachel Levinson-Waldman, *Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media*, 71 OKLA. L. REV. 997, 998 (2019) ("[P]olice are using social media not only to send information out to the public but also to keep track of what people are doing both online and off.").

[168] Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance,'* 9 U.C. IRVINE L. REV. 635, 638 (2019) ("[L]ocation information can be vital for pinning down a suspect to a crime scene or providing them with an alibi. Indeed, real-time and historical geolocation data has become a common piece of evidence collected in criminal investigations.").

[169] O'Toole, *supra* note 165.

[170] United States v. Jones, 565 U.S. 400, 403 (2012) (describing the use of GPS tracking technology).

[171] United States v. Lambis, 197 F. Supp. 3d 606, 609–11 (S.D.N.Y. 2016) ("[T]he Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator," colloquially known as a stingray device. (citing Office of the Deputy Attorney General, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, 2015 WL 5159600 (Sept. 3, 2015))).

[172] Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512 (2021).

[173] United States v. Tuggle, 4 F.4th 505, 510–11 (7th Cir. 2021) ("Tuggle's case presents an issue of first impression for this Court: whether the warrantless use of pole cameras to observe a home on either a short- or long-term basis amounts to a 'search' under the Fourth Amendment."), *cert. denied*, 142 S. Ct. 1107 (2022); *see also id.* ("Together, the three cameras

pattern matching might identify an individual in a crowd or among a database of suspects.[174] These investigatory superpowers can be used to develop evidence against individuals suspected of criminal wrongdoing.

Finally, in the trial context, digital technologies are being used as evidence to prosecute criminal activities.[175] While many of the above surveillance technologies exist in a pre-evidence state—helpful for identifying a suspect, but not necessarily used for trial proof—some technologies are being introduced in trial.[176] For example, the Baltimore Police Department piloted "Persistent Surveillance Planes" that could fly over the city and record all vehicle and pedestrian movements using powerful digital cameras.[177] The footage captured images every second and could be connected to other ground-level surveillance systems, allowing analysts to roll back the tape and watch events after the fact.[178] The evidence could then be provided to prosecutors for use at trial.[179] Forensic trial evidence now

---

captured nearly eighteen months of footage by recording Tuggle's property between 2014 and 2016.").

[174] *See* Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/8YEV-WS5Z]; *see also* Kate Kaye, *Police Can Use Facial Recognition Again After Ban in New Orleans, Home to Sprawling Surveillance*, PROTOCOL (July 26, 2022), https://www.protocol.com/enterprise/new-orleans-surveillance-facial-recognition [https://perma.cc/3GD2-W6CA].

[175] *See* SEAN E. GOODISON, ROBERT C. DAVIS & BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM 1, 7 (2015), https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf [https://perma.cc/TK3G-P63T].

[176] *See id.*

[177] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333–34 (4th Cir. 2021) (en banc) ("The AIR program uses aerial photography to track movements related to serious crimes. Multiple planes fly distinct orbits above Baltimore, equipped with PSS's camera technology known as the 'Hawkeye Wide Area Imaging System.' The cameras capture roughly 32 square miles per image per second. The planes fly at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day, weather permitting.").

[178] *Id.* at 334 ("The planes transmit their photographs to PSS 'ground stations' where contractors use the data to 'track individuals and vehicles from a crime scene and extract information to assist BPD in the investigation of Target Crimes.' 'Target Crimes' are homicides and attempted murder; shootings with injury; armed robbery; and carjacking. Between 15 and 25 PSS contractors analyze the data, working in two shifts per day, seven days per week." (citation omitted)); *id.* at 342 ("[T]he program enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield 'a wealth of detail,' greater than the sum of the individual trips." (citation omitted)).

[179] ANDREW R. ET AL., RAND, EVALUATING BALTIMORE'S AERIAL INVESTIGATION RESEARCH PILOT PROGRAM: INTERIM REPORT 10–11 (2021) ("[T]he final product from the AIR analysis was to be an evidence package—a briefing that would include aerial imagery, tracks, and annotations about suspects' behaviors and activities; video collected from CitiWatch cameras; images of buildings or locations drawn from Google Street View; and other information the AIR analysts could assemble on the people, vehicles, and locations related to the investigations. These evidence packages would be uploaded to the BPD's electronic

routinely includes gunshot detection data, cell-phone location data, and of course DNA evidence.[180] In addition, data from police worn body cameras and ALPRs have been admitted into evidence in criminal prosecutions.[181]

The above list of new technologies is necessarily incomplete, but such a list does offer a window into the potential changes to police surveillance power. At a minimum, the difference in scope and scale of emerging technologies can be identified. At a gut level, it is easy to see that there is a difference between a plane flying over a single backyard, and a plane that can record all the backyards in a city. It is easy to visualize that a beeper tracking one car is different than GPS satellites tracking all cars, or that a single CCTV camera is different than a network of tens of thousands of linked cameras.

The next Part will address why these different types of digital surveillance technologies warrant a new Fourth Amendment analysis.

B. *Why Digital is Different*

This Article seeks to contribute a specific argument to the larger debate around how the Fourth Amendment fits into the future of big data policing. I argue that the analog cases of the 1960s–1980s are so different from the policing technologies now in use, that they should no longer be relied upon to address the privacy and security threats posed by the new digital surveillance capabilities. In other words, the fact that police could once "constitutionally" do something with old technology is no longer license to make the same constitutional argument with new technology. This Part looks at three differentiating characteristics of new digital technologies that all share one similarity—they would be impossible for humans to do without technological, digitally-enhanced superpowers.

The importance of this analog/digital differentiation cannot be overstated. Despite clear differences in technologies and the passage of time, courts still rely on analog cases to justify Fourth Amendment outcomes in new technology

---

evidence management system, Evidence.com, where they would be available to detectives, their supervisors, and prosecutors and defense attorneys.").

[180] *See, e.g.*, Veronique Greenwood, *New Surveillance Program Listens for Gunshots, Get Police There in Minutes*, DISCOVER (May 30, 2012), https://www.discovermagazine.com/technology/new-surveillance-program-listens-for-gunshots-get-police-there-in-minutes [https://perma.cc/QA5A-HR53]; State v. Hill, 851 N.W.2d 670, 690–91 (Neb. 2014) (allowing Shotspotter evidence to be introduced into trial); Commonwealth v. Wilkerson, 156 N.E.3d 754, 767 (Mass. 2020) (discussing the admissibility of CSLI evidence); Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1261 (2016) (discussing DNA evidence).

[181] *See, e.g.*, United States v. Gibson, 366 F. Supp. 3d 14, 17 (D.D.C. 2018) (discussing the use of body-worn camera footage as evidence); Commonwealth v. McCarthy, 142 N.E.3d 1090, 1095–96 (Mass. 2020) (automated license plate readers).

cases.[182] The trial court in *Beautiful Struggle v. Baltimore* (aerial surveillance),[183] the appellate court in *Tuggle v. United States* (pole cameras),[184] and Justice Anthony Kennedy in his *Carpenter* dissent (CSLI),[185] all analyzed modern digital surveillance questions through an analog lens as if there was no difference in the technologies at issue. In fact, many courts when faced with a new surveillance technology go back to the world of beepers and cassette tapes to address the threats of artificial intelligence and structural sensor surveillance.[186] This default needs to change because the technological capacities of digital policing have changed.

This Part argues for that new way of thinking. First, this Part will look at "the act" of surveillance, demonstrating that what police are doing is actually different than what had been done in the past.[187] Next, this Part will look at "the result" of the surveillance, showing how what police get from these systems of surveillance is different in scale, scope, and usability. Finally, this Part will examine the scalability problem that comes from upgradable, interoperable, and privatized surveillance systems that did not exist in prior eras. The simple point being that the capabilities of today cannot find strong support in past police surveillance practices and need a new analytical starting point.

1. *The Act*

Digital technologies alter the act of surveillance.[188] In allowing for a broader, deeper, faster, cheaper, more accurate, automated, and aggregated process of over-

---

[182] *See, e.g.*, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 712–14 (D. Md. 2020), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

[183] *Id*. at 702, 712–14.

[184] United States v. Tuggle, 4 F.4th 505, 511, 513 (7th Cir. 2021) ("Ultimately, bound by Supreme Court precedent and without other statutory or jurisprudential means to cabin the government's surveillance techniques presented here, we hold that the extensive pole camera surveillance in this case did not constitute a search under the current understanding of the Fourth Amendment."), *cert. denied*, 142 S. Ct. 1107 (2022).

[185] Carpenter v. United States, 138 S. Ct. 2206, 2223–24 (2018) (Kennedy, J., dissenting) ("This case involves new technology, but the Court's stark departure from relevant Fourth Amendment precedents and principles is, in my submission, unnecessary and incorrect, requiring this respectful dissent.").

[186] *See, e.g.*, *Leaders of a Beautiful Struggle*, 456 F. Supp. 3d at 712–14 (D. Md. 2020); *Tuggle*, 4 F.4th at 514–16 (7th Cir. 2021); *Carpenter*, 138 S. Ct. at 2216–17 (2018). *See generally* Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1791 (2022) (discussing cases post-*Carpenter* that rely on traditional analysis to analog precedent).

[187] Analysis of how "the act" of digital surveillance is different than traditional surveillance was more thoroughly addressed in a previous article that focused on digital persistent surveillance technologies. *See* Ferguson, *Persistent Surveillance*, *supra* note 12, at 13–21.

[188] In a previous article I made a more detailed argument that several factors changed "the act" of persistent digital surveillance. *See id.* ("[A]ll digital persistent surveillance shares six attributes that differentiate what is happening from traditional police surveillance (and

collection of personal data, *the thing* that is happening is far different from a singular or simple collection of particularized information that human officers attempted in the past.[189] In contrast to police actions in the traditional Fourth Amendment canon,[190] the scale, speed, scope, and sophistication of information collection all look different because of the digital technologies at issue.

For one thing, digital surveillance, be it always-on video cameras, ubiquitous sensors, or continuously generating signals, shifts the focus from a singular, discrete search act to an automatic, continuous series of acts. The technologies are automatically always searching.[191] This non-human, automated reality upends traditional Fourth Amendment analyses.[192] Compared to the single overflight in *Ciraolo*, how many search acts were conducted with a twelve-hour flight taking one photo a second over Baltimore?[193] Tens of thousands? The automatic nature of the collection process complicates the identification of when the search occurs. Notice that automation does two things. One, it allows for capabilities that no human could do at scale (i.e., watch a city all at once for twelve hours). Two, it exposes the reality that these types of digital searches are

---

the case law developed around that human monitoring). Because all digital persistent surveillance technologies involve increased (1) automation, (2) acceleration; (3) accuracy; (4) accumulation; (5) aggregation, and (6) actualization of data—the resulting surveillance capacity is in fact different from the traditional analog equivalent." (footnote omitted)). While persistent surveillance and digital surveillance are not synonymous, a similar reasoning holds.

[189] *See* Hartzog, Conti, Nelson & Shay, *supra* note 22, at 1779–80 ("[A]utomated systems are highly efficient, which can reduce the cost of surveillance, analysis, and enforcement to negligible levels per incident. Manual surveillance, analysis, and enforcement require manpower, money, and time. Automation can be centralized, cheap, and virtually instantaneous." (footnote omitted)).

[190] *See* Nirej Sekhon, *Catchall Policing and the Fourth Amendment*, 71 DUKE L.J. ONLINE 111, 116–17 (2021) (describing the Fourth Amendment canon).

[191] This always on capability for surveillance has become commonplace in the consumer space. *See* Allison S. Bohm, Edward J. George, Bennett Cyphers & Shirley Lu, *Privacy and Liberty in an Always-On, Always-Listening World*, 19 COLUM. SCI. & TECH. L. REV. 1, 6 (2017) ("An always-on device is a consumer product with one or more electronic sensors capable of collecting and responding to audio, video, and other information-dense data. Always-on devices usually stream portions of that data to a remote party via the Internet, either intermittently or continuously. Always-on devices may be single purpose, such as voice-activated light bulbs, or general purpose, like the Amazon Echo and Google Home. In addition to in-home appliances, products like cell phones and Internet-connected cars can be considered always-on devices. Today, a majority of Americans own smartphones, equipped with GPS and mobile Internet connection, which are capable of streaming continuous location data to remote parties. Always-on devices are not just the future: they are the present.").

[192] *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 615 (2011) (describing how automation may complicate the traditional Fourth Amendment calculus based on human actions).

[193] *Compare* California v. Ciraolo, 476 U.S. 207, 209 (1986), *with* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 335 (4th Cir. 2021) (en banc) ("BPD initially continued storing the data that it had retained to that point; 1,916.6 hours of coverage comprised of 6,683,312 images.").

continuous and permeating, blurring the line between an easily identifiable government search act and the reality of continuous search acts.

Similarly, the speed of data capture allows for exponentially more data to be collected than in any previous era (and certainly compared to any human).[194] This ease of collection changes not only how data gets collected but what gets collected (including public and private information).[195] One of the realities of new always-on surveillance technologies is that they are over-broad, capturing innocent conduct along with occasional illicit acts.[196] The planes flying over Baltimore captured everything from political protests to private walks to violent crime.[197] Such a capacity is not something that human officers would or could do without the speed, ease, and cost-savings of digital technology.

The acceleration and accumulation of information results in the ability to aggregate data across different datasets.[198] Not only is there more data being collected, but studying the collected data can offer more revealing inferences and insights about the people involved.[199] What a police officer might see flying over one home is much less than that a police officer flying over that home every day, or seeing the other homes that the resident goes to (and with whom). This is not just a function of how the data is used (as will be discussed in "the result"

---

[194] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 75 (2013) ("Information gathering is faster, cheaper, and more comprehensive than ever before. Whereas information gathered by public and private entities once tended to remain in information silos, it is now seamlessly shared with countless organizations via the Internet."); Meg Leta Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18 VAND. J. ENT. & TECH. L. 77, 85 (2015) ("Digital automation utilizes elegant algorithms to process piles and piles of data to some end.").

[195] *See* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2324 (2007) ("Widespread private deployment of networked sensors is inevitable, because it rests on several powerful technological trends that are unlikely to be reversed. The four primary elements of the pervasive surveillance web are cameras, wireless sensor networks, networked devices incorporating location data, and tools for information sharing and aggregation.").

[196] In fact, one could argue that most of the collected video footage and sensor data involves non-criminal activities. *See* Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1, 9 (2013).

[197] The Plaintiffs in the Baltimore case sued to protect their right to associational liberty and to conduct political protests free from aerial surveillance. *See* Brief for Plaintiffs-Appellants at 15–17, 19–22, 47, *Leaders of a Beautiful Struggle*, 2 F.4th 330 (No. 20-1495).

[198] *See* Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289, 289 (2015) ("Data aggregation has played a role in three recent cases implicating one's reasonable expectation of privacy under the Fourth Amendment. Although the cases involve disparate doctrines, they all focus on aggregation as a reason to depart from prior law.").

[199] Gray & Citron, *supra* note 194, at 75 ("Aggregation technology and advanced statistical analysis tools have enhanced the capacities of those who wield surveillance technology to know us, often in ways that we do not know ourselves.").

Part next), but how it is collected.[200] The act of building an aggregated dataset is a different thing from collecting a single-source dataset.

Finally, the technologies offer a more accurate collection of data.[201] While mistakes will occur, the ability to see more, collect more, and analyze more overshadows any human limits to see, hear, and process large amounts of usable information.[202] Increased accuracy, of course, does not mean without error. The data collected comes with the biases of those who choose what data to collect, what to ignore, and almost always replicates existing inequalities in society.[203] Yet, what is captured in the camera lens can be more accurate than the same information collected by humans who also are equally blinded by biases, lacuna, and structural discriminatory practices.[204] "Where" the cameras point their lens

---

[200] This concept has been known as the mosaic theory of surveillance, recognizing that the sum of digital clues can be more revealing than the individual parts. *Cf.* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1810–12, 1834 (2014); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012).

[201] The term "accurate" is obviously contestable as most digital collection of information is rife with error, and also suffers from more structural infirmities about the types of data collected, the selection process, the cleansing of data, and other systemic challenges that arise with the collection of vast amounts of real-world information. For example, in the facial recognition context, it has been revealed that initial high accuracy claims about face matching was only true for a small subset of faces (white men), and was, in fact, inaccurate when applied to anyone else (women, non-white people). Yet, those selling the technology could claim "accuracy" when in fact the structure of testing "accuracy" was biased and misleading due to its selective testing. *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 1–2 (2018); Sophie Bushwick, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, SCI. AM. (Dec. 27. 2019), https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/ [https:// perma.cc/2UCR-72ZQ] ("NIST's tests revealed that many of these algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one. In searching a database to find a given face, most of them picked incorrect images among black women at significantly higher rates than they did among other demographics."); *see also* Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7. 2019), http://time.com/5520558/artificial-intelligence-racial-gender-bias/ [https://perma.cc/6UWF-7DE3]; Clare Garvie & Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [https://perma.cc/36RG-XBVE].

[202] *See* Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043, 1061 (2019) ("[C]hanges in the speed and accuracy of queries effect a step change in the quality of surveillance-based evidence available to police.").

[203] *See* Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 OHIO ST. J. CRIM. L. 503, 513–17 (2018) (discussing racial bias in policing technologies); *see also supra* note 201 (discussing the errors in facial recognition technology).

[204] This may also be a contestable point as there have been debates about the accuracy of police body camera footage and the technologies that provide it. *Compare* Caren Myers

unquestionably will be the product of systemic biases (in most jurisdictions), but "what" the camera captures in that lens will be a more accurate image than a human recounting of the same observation.

In sum, what the police are doing when they are conducting digital surveillance operations is different than prior police surveillance acts. This, of course, does not mean the surveillance act is unconstitutional (or constitutional) under the Fourth Amendment, but only makes the point that analogies to pre-digital precedent hold little persuasive power. A new analysis must emerge to address the changes arising from digital surveillance.

2. *The Result*

What police are doing when they conduct digital surveillance is different, but so is the result of that surveillance. Front-end data collection is far less important than back-end data analytics.[205] In fact, one of the most significant changes that emerges from digital surveillance is the immense datasets that get created by the always-on collection systems.[206] As the Supreme Court recognized in *Riley*, digital collections of personal information allow for a quantitively and qualitatively different end product for investigators.[207] The result of what you get is just vastly deeper, broader, thicker, and more revealing.

Most importantly, this richer dataset of stored personal information allows for retrospective investigatory searches.[208] This search capacity is different for two distinct reasons. First, the stored datasets are filled with vast amounts of

---

Morrison, *Body Camera Obscura: The Semiotics of Police Video*, 54 AM. CRIM. L. REV. 791, 812 (2017) ("There is little point in claiming that any one type of police video evidence—dash camera, body camera, surveillance camera—is 'better' or 'more accurate' than another, since a useful recording is always a question of luck, lighting, and position."), *with* Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 U.C. DAVIS L. REV. 897, 903 (2017) ("Body cameras record events closer up, yielding more detail than ever before captured by testimony or a dash camera.").

[205] *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 365 (2015) ("To solve crimes, law enforcement must not only collect information, but also identify and link individuals to their accumulated data. In short, data must be connected with identifiable human beings.").

[206] Rushin, *supra* note 196, at 11 ("[I]ndiscriminate data collection allows law enforcement to aggregate large amounts of information about a single individual, thereby revealing personal information about habits and behaviors."); Bohm, George, Cyphers & Lu, *supra* note 191, at 6.

[207] Riley v. California, 573 U.S. 373, 393 (2014).

[208] *See* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 572 (2017) ("When surveillance technologies record while they watch, therefore, courts must be alert to the risk that those recordings offer both a ready-made mosaic and a virtual time machine, available for after-the-fact review and exploitation, and law enforcement must be alert to the risk that their surveillance poses to Fourth Amendment rights.").

personal data.[209] In all the old search cases (a telephone conversation, a few photographs, a thermal heat reading) the data collection was thin.[210] While the collected evidence was valuable to the prosecution (because it proved facts about a crime), it did not reveal much else at all and was not used for other prosecutions or purposes.[211] Second, the technical ability to mine the data in the traditional cases was not very powerful.[212] Because the nature of the collection was limited, the ability to reveal personal data or patterns of behavior was equally limited.[213] In contrast, for example, the collected images of Baltimore is far more revealing in terms of what can be mined for evidence.[214] Again, the resulting collection of searchable and predictive data is something largely impossible for humans to replicate and only available because of powerful computer and analytical capacities.[215]

Equally problematic, these stored datasets are revealing about associational choices, political activities, and personal identity.[216] Continuing with the Baltimore example, analysts had 45 days of travel patterns and public activities of everyone who entered Baltimore, and could combine that information with ground-level camera systems, automated license plate readers, and other mapping technology.[217] For example, using the technology, one could identify a church,

---

[209] Rushin, *supra* note 196, at 11; *see, e.g.*, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 703–05 (D. Md.), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

[210] *See* Katz v. United States; 389 U.S. 347, 348 (1967); Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986); Kyllo v. United States, 533 U.S. 27, 29 (2001).

[211] *See, e.g.*, *Katz*, 389 U.S. at 354. For example, the phone calls recorded to be used against Charlie Katz were limited to one investigation. *Id.* While, of course, they could be used for related cases, the collection was quite different than collecting all the phone calls from an area or being able to search through all the collected phone calls of a person.

[212] *See, e.g.*, *Dow Chem. Co.*, 476 U.S. at 238–39.

[213] *See Katz*, 389 U.S. at 354; *Dow Chem. Co.*, 476 U.S. at 238–39.

[214] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 342 (4th Cir. 2021) (en banc) ("[T]he program enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield 'a wealth of detail,' greater than the sum of the individual trips." (citation omitted)); s*ee also* United States v. Tuggle, 4 F.4th 505, 511 (7th Cir. 2021) (describing the 18 months observation of the house), *cert. denied*, 142 S. Ct. 1107 (2022).

[215] *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 107 (2018) ("One of the goals is to find patterns in big data sets—for example, the places and times crime is most likely to occur—and to generate predictive models to guide the allocation of public services—for example, how and where to police.").

[216] *See Leaders of a Beautiful Struggle*, 2 F.4th at 341–42 (discussing the wealth of information that can be determined from continual surveillance).

[217] *See id.* at 334 ("Further, PSS may 'integrate . . . BPD systems' into its proprietary software 'to help make all of the systems work together to enhance their ability to help solve and deter crimes.' The PSA lists BPD's dispatch system, 'CitiWatch' security cameras, 'Shot Spotter' gunshot detection, and license plate readers as systems to be integrated. As a result,

or gun range, or methadone clinic and track all the people who left that particular building to their homes. Again, because home addresses are easily obtainable with mapping software, the systems can indirectly reveal identity (and by inference activity).[218] License plate readers and street-level cameras can also help confirm the identity of individuals (if, for example, many people shared a house).[219] Any pattern of activity—even those protected by First Amendment principles—would be vulnerable to identification because of the stored datasets in police possession.[220] Again, the surveillance power is not just the video, but how the video can be used in combination with other surveillance systems filled with personally identifiable information in a searchable database.[221]

While the Supreme Court in *Carpenter* and *Jones* recognized the privacy harm in creating expansive and retrospectively searchable databases of location information,[222] this focus on access to large datasets was absent in early Fourth Amendment cases because that level of data collection was technologically impossible. Simply stated, because older technology and human observers were unable to collect the volume of data now available, and because the algorithms did not exist to sort through the data in usable form, the resulting investigative datasets never appeared as a constitutional issue.

In saying that *the result* of digital surveillance is different, I am also saying that the potential power to search the data creates different privacy harms. Inherent in the possession of searchable datasets is a power to investigate, intimidate, and control dissent in a community.[223] The thing police have as a

---

AIR reports may include ground-based images of the surveilled targets from 'the cameras they pass on the way.'" (citations omitted)).

[218] *See* MORRAL ET AL., *supra* note 179, at ix ("Using aerial imagery, analysts would construct annotated tracks displaying the paths traveled by people and vehicles through the city before and after a crime, noting when suspects or witnesses appeared to spend time with cars, other vehicles, or in homes or buildings. When people or vehicles were seen to pass CitiWatch cameras or license plate reader systems, AIR analysts would use those systems to download video or license plate information that could help to identify cars, drivers, passengers, or pedestrians of interest.").

[219] *See id*.

[220] Brief for Plaintiffs-Appellants, *supra* note 197, at 1 (raising both First Amendment and Fourth Amendment objections to the surveillance planes).

[221] *See* Katelyn Ringrose & Divya Ramjee, *Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy*, 11 CALIF. L. REV. ONLINE 349, 360 (2020) (discussing facial recognition surveillance and political protest).

[222] *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("The government can store such records and efficiently mine them for information years into the future." (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc))); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("[W]hen the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.").

[223] *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 434 (2008) ("Government surveillance—even the mere possibility of interested watching by the state—chills and warps the exercise of this interest. This effect was understood by the drafters of the Fourth

result of collecting so much information is a different power than what they had previously. Therefore, applying old-fashioned constitutional analysis to new privacy threats misapprehends the privacy and security concerns arising from new searchable systems that can be weaponized by government investigators.

3. *Scale and Scalability*

Big data policing is in its relative infancy. The data-driven technologies discussed throughout this Article are still developing, many in pilot programs or just getting adopted across jurisdictions.[224] Even the discussion of the surveillance capabilities as discrete technologies is a bit misleading. A more accurate description would see these specific policing tools (cameras, sensors, datasets) as part of growing systems of data-driven surveillance.[225] As the technologies scale, issues of how the technologies will become interoperable, upgradeable, and more like networked platforms will become more pronounced.[226]

Scalability, interoperability, and upgrades are all related problems that have no parallel in traditional surveillance practices. For example, the Baltimore aerial camera planes (already an upgrade from ordinary aerial surveillance) were not planned as stand-alone surveillance tools.[227] First, in terms of coverage, the city planned to fly three wide-angle surveillance planes a day.[228] But, of course, there was no technological or legal limit to the number of planes that could have been deployed to cover the area.[229] The scale was only limited by money and political will.[230]

Amendment, who grasped the relationship between preventing government searches of papers and protecting religious and political dissent.").

[224] *See, e.g.*, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333 (4th Cir. 2021) (en banc) (describing the "new aerial technology" used for surveillance in Baltimore).

[225] *Cf.* Ferguson, *Sensor Surveillance*, *supra* note 10, at 79–80 ("[A]long the continuum of data collection available with smart sensors, the Fourth Amendment is most concerned about arbitrary, permeating, aggregating, permanent, and individualized systems of surveillance.").

[226] *See generally* Elizabeth E. Joh & Thomas Wuil Joo, *The Harms of Policy Surveillance Technology Monopolies*, DENV. L. REV. F. (forthcoming 2022), https://papers.ssrn.com/sol3/papers.cfrn?abstractid=3834777 (discussing the role of policing platforms).

[227] POLICING PROJECT, *supra* note 160, at 8 ("[T]he use of information from ground-based surveillance technologies—such as red-light cameras, automated license plate readers (ALPRs), and CitiWatch cameras—both assist in tracking and are critical to helping analysts find identifying information about a specific car or individual. This is why the aerial, ground-based, and human resources should be thought of as one composite system.").

[228] *See* Brief for Plaintiffs-Appellants, *supra* note 197, at 1 (describing the plan to fly three planes over the city).

[229] The original agreement was for a limited number of planes, but without a constitutional or statutory limit, the city could have added more planes as they wished. *Id.* at 5–14.

[230] Money and political will, of course, are limiting factors for most surveillance technology, but the point is that there are no legal or constitutional limits.

Equally importantly, the program was designed to work with other police datasets.[231] By design, PSS analysts were supposed to get access to automated license plate readers, gunshot sensors, street-level cameras, and police databases.[232] The idea was to take one information stream and augment it with other police data streams to enhance police investigative power.[233] In theory, this interoperability has no limit, as any existing government dataset could have been fed into the system. Federal fusion centers, the NYPD's Domain Awareness Center, and the LAPD's Palantir system provide good examples of broadly interoperable systems that can vacuum up many different sources of data for police investigatory purposes.[234] Such locally grown surveillance command centers are sprouting up even in smaller cities.[235]

Finally, most digital systems—like most computer systems—can be upgraded with additional capabilities.[236] In other words, current internally-imposed limits on use or technical constraints can change if police departments choose to improve their surveillance capabilities.[237] While the Baltimore aerial cameras purposely limited the granularity of video data so as to not capture

---

[231] *See* POLICING PROJECT, *supra* note 160, at 8; Koops, Newell & Škorvánek, *supra* note 168, at 638.

[232] *See* POLICING PROJECT, *supra* note 160, at 8; Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021) (en banc).

[233] *See* POLICING PROJECT, *supra* note 160, at 8.

[234] *See generally* Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. L. & SOC. SCI. 293, 295–301 (2018) (discussing both Domain Awareness Systems and Palantir's social network analysis systems).

[235] Andrew Guthrie Ferguson, *Big Data Policing Is Coming to Small Towns. There's a Reason Big Cities Rejected It.*, NEWSLEADER, https://www.newsleader.com/in-depth/opinion/2021/03/22/big-data-policing-coming-your-town-theres-reason-failed-big-cities/4614693001/ [https://perma.cc/8B9Q-4JXP] (Mar. 23, 2021).

[236] Steve Symanovich, *5 Reasons Why General Software Updates and Patches Are Important*, NORTON (Jan. 23, 2021), https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html [https://perma.cc/5V4A-2X6Z] ("Updates can add new features to your devices and remove outdated ones.").

[237] As but one example, ISMI catcher's (StingRay devices) can be upgraded from the initial capacity to find a particular phone, to other more invasive capabilities. *See* Jenna Jonassen, *StingRays, Triggerfish, and Hailstorms, Oh My! The Fourth Amendment Implications of the Increasing Government Use of Cell-Site Simulators*, 33 TOURO L. REV. 1123, 1132–33 (2017) ("StingRay devices are known to force *all* cell phones in the area of the cell tower to send their identification information to the device. Since the machine is only able to detect a particular cellular phone's identification once it registers with a network, the device must search and collect information from *every* in-range cellular device before it can actually pinpoint the targeted user. Some upgrades to the StingRay machines make their functionality even more intrusive–software upgrade 'FishHawk' allows users to listen to conversations without the cellular user's knowledge, while the 'Porpoise' upgrade can be installed to provide dual-functionality for surveillance of both location and incoming and outgoing text messages." (footnotes omitted)).

faces, this internal rule could have been modified.[238] It was the internal policy, not the technology that added privacy protections. Similarly, while the Baltimore cameras did not utilize facial recognition technology, any sophisticated video system is an upgrade away from adopting it.[239] In fact, many digital police surveillance systems are better thought of as digital platforms and thus can add or limit capabilities with a change in policy or software.

Again, in an analog world of simple surveillance tools, questions around scale or interconnectedness or future upgrades to systems were never raised. No one was trying to add a dataset of other information to a beeper, pen register, or cassette tape.[240] Tools were tools. But when tools become systems and systems become networked, the capabilities change. The result is that today's courts must be mindful of growing surveillance power limited only by internal policy decisions or assumptions about the current capacity of the technology. Digital policing technology is different, not simply because of what it is, but also because of what it can become.

C. *Expectations and Digital Policing*

To say digital policing is different than traditional police surveillance is to acknowledge that something new is happening. What police are doing, what they are getting, and the boundless nature of how the surveillance systems can all expand in scale and scope represents a different problem set than seen in earlier eras.

The simple goal of this Article is to draw that line of difference clearly in the doctrinal sand. The more complex question is what to make of the changes. If digital is different when it comes to new policing technologies, how should those technologies impact current Fourth Amendment law? Does a "reasonable

---

[238] The choice to limit the capabilities of the cameras was in an effort to address privacy concerns. *New Technology Initiatives*, BALT. POLICE DEPARTMENT, https://www.baltimorepolice.org/resources-and-reports/new-technology-initiatives [https://perma.cc/WQS7-6JVJ] (Nov. 17, 2022); Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 704 (D. Md.) ("The imagery is limited to '1 pixel per person'—essentially, a single dot on the map. Accordingly, an individual's characteristics are not observable In the images." (citations omitted)), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

[239] For example, the camera system in Detroit could be upgraded to include facial recognition. *See Project Green Light Detroit*, CITY OF DETROIT, https://detroitmi.gov/departments/police-department/project-green-light-detroit [https://perma.cc/ZX77-UHH9]; *see also, e.g.*, Natasha Lomas, *London's Met Police Switches on Live Facial Recognition, Flying in Face of Human Rights Concerns*, TECHCRUNCH (Jan. 24, 2020), https://techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facial-recognition-flying-in-face-of-human-rights-concerns [https://perma.cc/Y9QR-L7E6].

[240] The reason for this, of course, is that the then existing, non-digital technology did not easily allow such interconnection. The technologies were stand-alone mechanical or physical tools which did not allow for easy integration with larger systems.

expectation of privacy" make sense in a world without much digital privacy and largely dependent on third-party digital providers?[241] Does *Carpenter* offer a new Fourth Amendment test?[242] Are there other future proofing principles that might help guide courts to an answer?[243] These questions are big, and complex, and without easy answers.

Many scholars have tried their hands at offering a Fourth Amendment solution to the puzzle of digital surveillance.[244] This Article does not seek to offer yet another Fourth Amendment theory about expectations of privacy in a digital world, but simply offers one insight that arises from carefully comparing the old analog surveillance cases to new big data policing innovations—namely the central role of human limits in shaping expectations of privacy.

One of the most striking realizations in studying the early Fourth Amendment cases is how dependent the surveillance was on human agents (and agency). Whether it is the *Katz* officers physically taping the microphones on the telephone booth and turning on the device,[245] or the *Karo* agents tracking the beeper,[246] or police officers peering out of planes to see marijuana growing,[247] the human was not only in the loop, but was key to the search. While the cases were nominally focused on technology and the Fourth Amendment, the reasonable expectations of privacy was still a reaction to human observation.

This insight matters because it shaped how individuals could expect privacy and could react to the threat of police surveillance. If the technology really only

---

[241] This is not a new Fourth Amendment question. *See, e.g.*, Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 568 (2016); David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH L. REV. 189, 190–91 (2015); Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 24–25 (2013); Gray & Citron, *supra* note 194, at 64, 67; Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1334–36 (2012); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479–80 (2011); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 322–23 (2002).

[242] *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 390 (2019); *see also* Matthew Tokson, *The* Carpenter *Test as a Transformation of Fourth Amendment Law*, U. ILL. L. REV. (forthcoming 2022) (manuscript at 3–4), https://ssrn.com/abstract=4094166 [https://perma.cc/WZ5Y-KXW5].

[243] *See* Ferguson, *Future-Proofing*, *supra* note 17.

[244] The question of designing a Fourth Amendment theory for the digital age has been addressed by many scholars. Brilliant scholars like Orin Kerr, Danielle Citron, David Gray, Mathew Tokson, Jeffrey Bellin, Laura K. Donohue, Shima Baradaran Baughman, Bennett Capers, Sheryll Cashin, Tracey Maclin, James J. Tomkovicz, Daniel J. Solove, Elizabeth E. Joh, Margaret Hu, David A. Sklansky, Stephen E. Henderson, Christopher Slobogin, Paul Ohm, Ric Simmons, Marc J. Blitz, Rebecca Lipman, Andrew Selbst, and Kiel Brennan-Marquez have all tried their hand at theorizing a new way forward around the Fourth Amendment and new technologies.

[245] Brief for Petitioner, *supra* note 23, at 5.

[246] United States v. Karo, 468 U.S. 705, 708 (1984).

[247] California v. Ciraolo, 476 U.S. 207, 209 (1986).

provided information that human agents could obtain (in public), then individuals could act accordingly to preserve a measure of privacy.[248] It meant individuals could erect a literal or metaphorical curtilage wall to guard their private lives.[249] It meant individuals could take precautions to avoid being overheard or watched or followed. As long as a human agent had to be in the loop of surveillance, "the watched" could protect their privacy from "the watchers" and could expect a court to rule accordingly.

Further, the more superpower-like the surveillance grew (and thus less human), the more restraints the Supreme Court put on police. Super-hearing capabilities in *Katz*,[250] or seeing through walls in *Kyllo* provided super-human powers that required constitutional restraint.[251] Again, the farther away one got from the type of human-powered surveillance that people could expect and protect against, the more the courts were willing to protect privacy.

Digital policing technology that operates without humans is disconnected from these original limitations and expectations. Systemic surveillance, fueled by artificial intelligence, pattern matching, and other automated algorithmic suspicion

---

[248] More intriguingly, the human focus of older cases exposes one of the doctrinal missteps that has had profound impacts on confusing Fourth Amendment search cases. While likely worthy of its own article, it is worth noting here how the original "expectation of privacy" test conflates expectations of privacy from police with expectation of privacy from everyone else. At the time *Katz v. United States*, 389 U.S. 347 (1967), was decided, and when Justice Harlan was writing about what people expose to others, the observational/surveillance capabilities of police and ordinary people were basically the same. So, when a court said an individual had an expectation of privacy in their call or home or papers, it meant an expectation of privacy from either other people or police with no differentiation needed. Because the technology (microphone with tape cassette equivalent) was not much different than a person listening in, the Supreme Court could equate expectations from others and expectations from police. Individuals could also act accordingly knowing the physical limitations of human surveillance. As long as they acted to protect against other humans, the Court was inclined to protect their expectation. Digital policing and new surveillance technologies exposes the conflation, because now police can do many more things that humans cannot do. One can take all the precautions in the world to protect conversations, papers, or activities from other human beings, but could still be monitored through new surveillance technology. In other words, expectations of privacy demonstrated against human surveillance, may do nothing to prevent government collection of personal data. This could mean that the expectations of privacy cannot exist in a world of advanced surveillance. Or it could mean that the legal test that conflates expectations of privacy from human surveillance and government surveillance cannot stand.

[249] I have spent some time developing the idea of "virtual" or "digital" or "informational" curtilage as a Fourth Amendment concept in a series of articles. *See* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1314–16, 1361–62 (2014) (virtual curtilage); Ferguson, *Internet of Things*, *supra* note 11, at 808–09 (digital curtilage); Ferguson, *Fourth Amendment*, *supra* note 11, at 617–18 (informational curtilage).

[250] *See* Brief for Petitioner, *supra* note 23, at 5.

[251] *See* Kyllo v. United States, 533 U.S. 27, 29–30, 34–36 (2001).

goes well beyond human capabilities. Something like an all-seeing spy plane creating datasets of millions of clues really has no human comparison.

The question is what to do with this new reality. It could mean that everyone loses all expectations of privacy because technology can see all. Or, it could mean that new expectations (or doctrines) must be established in response to technological threats. Scholars have debated some ideas, but the still unanswered question will center the Fourth Amendment debate for years to come.[252]

All this Article seeks to demonstrate is that digital policing is different enough that one must take this changed reality seriously as a matter of doctrine. What one could do in the past is not the same thing as what one can do in the future with big data systems. The technologies are different. The expectations of privacy are different. And, thus, Fourth Amendment doctrine must respect those differences.

IV. CONCLUSION

The theme of this symposium is *The Right of the People to Be Secure: Modern Technology and the Fourth Amendment*. One aspect of security is to make sure that the Fourth Amendment has relevance in the digital age. While a complete accounting of that conception of Fourth Amendment security is beyond the scope of this Article, one point is clear—the technologies of the 1960s, 1970s, and 1980s should not control the Fourth Amendment of the future.

Any honest accounting of the technologies and reasoning of those early Fourth Amendment cases shows why they cannot bear the analytical weight of upholding modern digital searches. While courts have borrowed and bent the precedent to try to fit it into the digital era, a true accounting of the inherent limits of cassette tapes, beepers, and microfilm as binding precedent to digital surveillance just falls apart under analysis.

This is not to say that analogies are always wrongheaded. Courts, limited by precedent and history, must try to adapt old principles to new problems.[253] The Supreme Court has taken creative liberties with its new digital surveillance theories to focus on harms that were simply not present in the analog age. *Carpenter* is a good example of a court attempting to find a framework for future Fourth Amendment protections.[254]

But *Carpenter* is also a good example of why Fourth Amendment law must separate itself from blindly following analog precedent. The beeper cases with their reliance on local human operators and limited public observations have no connection with the reality of a national cell network that can track everyone,

---

[252] *See supra* notes 244, 248 and accompanying text.

[253] *See* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 252–53 (2017) (discussing the limits of legal analogies with new policing technologies).

[254] *See* Ferguson, *Future-Proofing*, *supra* note 17.

everywhere, without human involvement.[255] It is not just the technology, but the logic of expectations of privacy that falls apart under analysis. Once courts have recognized the limitations of analogies, it opens up space to rethink the doctrine. To say digital is different is also to say the Fourth Amendment must be different.

For courts this must mean both interrogating the logic of the available analogies, and being courageous about developing new frameworks. First, courts must be precise in thinking through the technologies. In Baltimore, for instance, the trial court's legal reliance on a single plane flight in *Ciraolo* to justify a city-wide surveillance camera was too cursory.[256] Both involve flight, true, but as discussed in Part III, everything else in terms of act, scope, and result is different. The proper approach would be for the court to say that *Ciraolo* was not an appropriate analogy from which to make a legal conclusion.

This does not mean that courts are powerless to decide cases involving digital policing technologies like persistent surveillance planes. The *Katz*/*Carpenter* cases still provide a general framework for analysis. Courts may not get the balance right, but by shaking off the dust of old cases, they may find something new to address modern gaps in doctrine. The key is to have courage to recognize that something new is necessary. Expectations of privacy and claims of informational security are harder in the digital age, but courts have the tools to adapt to these new challenges. As I and others have written before, the Fourth Amendment can be interpreted to tackle the challenges of new forms of digital surveillance.[257]

The next challenge is to fill in the doctrinal gap, recognizing that Fourth Amendment security requires an accounting for changes in the act, result, and scalability problems discussed earlier. Digital surveillance is already changing policing—the still open question is how will it change the Fourth Amendment in the face of new technology.

---

[255] *See, e.g.*, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021) (en banc).

[256] *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 712 (D. Md.), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

[257] *See supra* notes 244, 248 and accompanying text.