ALMOST GONE: THE VANISHING FOURTH AMENDMENT'S ALLOWANCE OF STINGRAY SURVEILLANCE IN A POST-*CARPENTER* AGE

HARVEY GEE*

TABLE OF CONTENTS

* The author is an attorney in San Francisco. He previously served as an Attorney with the Office of the Federal Public Defender in Las Vegas and Pittsburgh, the Federal Defenders of the Middle District of Georgia, and the Office of the Colorado State Public Defender. LL.M, The George Washington University Law School; J.D., St. Mary's School of Law; B.A., Sonoma State University. The author thanks Taylor Francis, Elvira Razzano, Austin Smith, and the *Southern California Review of Law and Social Justice* for their assistance and hard work in the preparation of this article.

The Fourth Amendment[1] continues to erode. You can be pulled over while driving for just about any reason under the pretext that you violated a traffic law.[2] You can also be stopped while you are walking down the street in a "high crime area" and checked for an active arrest warrant.[3] Cops can also secretly track your location via your smart phone using cell-site simulators, known as Stingrays, that send powerful electronic signals to bait automatic responses from all nearby cell phones.[4]

This Article examines a Fourth Amendment that is now "vanishing" due to new surveillance technology, and narrowly focuses on how the changing Fourth Amendment jurisprudence implicates the secretive and unfettered use of Stingray technology.

This Article is divided into four Parts. The first two Parts provide the necessary groundwork for understanding how much the Fourth Amendment

---

[1] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[2] Whren v. United States, 517 U.S. 806, 813 ("Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis.").

[3] *See* Illinois v. Wardlow, 528 U.S. 119, 124 (2000) ("An individual's presence in an area of expected criminal activity, standing alone, is not enough to support a reasonable, particularized suspicion that the person is committing a crime. But officers are not required to ignore the relevant characteristics of a location in determining whether the circumstances are sufficiently suspicious to warrant further investigation.") (internal citation omitted).

[4] *See* Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FEDERALIST SOC'Y REV. 29, 30 (2016) (describing how Stingrays mimic cell phone towers, allowing authorities to use them to target devices and establish connectivity with law enforcement); Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185 (2014) ("[The Stingray] deceives nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the cell site simulator."); Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 144–45 (2013); Andy Martino, *Black Lives Matter Activists Are Convinced the NYPD Hacked Their Phones*, OUTLINE (Apr. 7, 2017, 1:30 PM), https://theoutline.com/post/1360/black-lives-matter-police-surveillance-the-cops-hacked-their-phones?.

has weakened in the past fifty years. Part I examines the lack of police accountability that is enabled and exacerbated by a weakened Fourth Amendment and addresses the ability of the police to pull over cars with near impunity. Part II explores the myriad ways in which law enforcement is able to exploit stop and frisks to create what is effectively an occupied police state in communities of color.

The last two Parts explore the future of the Fourth Amendment in the digital era. Part III reviews the Court's Fourth Amendment jurisprudence on surveillance technology leading up to *Carpenter v. United States*,[5] which shuttled the Fourth Amendment into the digital age.[6] It proceeds to analyze the *Carpenter* ruling, which provides much needed protections against technologically enhanced police surveillance powers,[7] and its implications for future privacy cases.

Part IV investigates the prevalent use of Stingray surveillance technology by law enforcement to spy on people. As much as stop and frisks create and sustain a physical police state, Stingray surveillance facilitates a *virtual* police state. Lacking guidance on this issue of law enforcement using portable Stingray cell-site simulators as digital surveillance tools, courts must choose to apply, adapt, or reject settled doctrinal rules, and interpret recent Supreme Court decisions, in deciding whether using Stingrays violate the Fourth Amendment. Until the Supreme Court addresses the issue of cell-site simulators by the police, state supreme courts and federal courts, in the interim, can adopt the reasoning of *Carpenter* and

---

[5] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[6] *See* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM) [hereinafter Kerr, *Understanding* Carpenter], http://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision (reporting that the "Court goes back to 'the critical issue' of 'basic Fourth Amendment concerns about arbitrary government power' that are 'wrought by digital technology.'"). While many privacy rights advocates celebrated the *Carpenter* ruling, there are some scholars who believe the decision does not go far enough. Professor Aziz Huq suggests that given the amount in which the Fourth Amendment has so heavily eroded, *Carpenter* will not as greatly affect police practices as one may initially think. Huq claims that because the probable cause requirement has been watered down to "fair probability," "*Carpenter*'s holding that a warrant is required to acquire cell-site locational data is likely to impose no great burden on the police" and will likely be "ineffectual in practice." *See* Aziz Huq, *The Latest Supreme Court Decision Is Being Hailed as a Big Victory for Digital Privacy. It's Not.*, VOX, www.vox.com/the-big-idea/2018/6/22/17493632/carpenter-supreme-court-privacy-digital-cell-phone-location-fourth-amendment (last updated June 23, 2018, 7:43 AM) (addressing *Carpenter*'s recognition of "a constitutional right to privacy in the locational records produced by your cellphone use.").

[7] Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment. *See also* Henry Gass, *Cell Signal: What High Court Ruling May Mean for Future of Digital Privacy*, CHRISTIAN SCI. MONITOR (June 22, 2018), https://www.csmonitor.com/USA/Justice/2018/0622/Cell-signal-What-high-court-ruling-may-mean-for-future-of-digital-privacy.

state court decisions which have ruled against the warrantless use of Stingrays for the necessary analytical framework. The article concludes by advocating for a warrant requirement for the use of Stingrays.

I. FOURTH AMENDMENT JURISPRUDENCE AND THE LACK OF POLICE ACCOUNTABILITY IN TRAFFIC STOPS

The Fourth Amendment was designed to be a counterweight to the authority of government agents armed with general warrants and writs of assistance to conduct broad and indiscriminate searches with impunity.[8] Because of this, it substantively proscribes violations of "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . ."[9]

In addressing the Fourth Amendment's reach and scope, the Court initially defined "search" and "seizure" solely as physical intrusions.[10] In time, Fourth Amendment jurisprudence has evolved with societal changes and technological advances. The Court now uses the reasonable expectation of privacy test from *Katz v. United States*[11] to determine whether a "search" under the Fourth Amendment has occurred. In *Katz*, the petitioner relied on the privacy of a phone booth when he made illegal gambling wagers, not knowing that federal agents had covertly attached an electronic listening and recording device to the outside of the booth.[12] The Court held that the Fourth Amendment protected the petitioner's oral statements.[13]

Under the *Katz* two-prong test, a search takes place when the defendant manifests an actual expectation of privacy that society is willing to

---

[8] DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 70–71 (2017). *See also* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602–1791*, *in* THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE 39–41 (Cynthia Lee ed., 2011) (describing how citizens have little protection from government overreach); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, *in* THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE, *supra*, at 34–35 (citing historical evidence indicating "that the Framers preferred use of specific warrants rather than warrantless intrusions" and wanted to prevent "unjustified searches and arrests from occurring."). The Fourth Amendment initially applied only to the federal government until the Court held that it is "incorporated" to the states via the Fourteenth Amendment). *See* Wolf v. Colorado, 338 U.S. 25, 33 (1949) (holding that "in a prosecution in a State court for a State crime[,] the Fourteenth Amendment does not forbid the admission of evidence obtained by an unreasonable search and seizure," meaning that states can develop their own remedies for Fourth Amendment violations).

[9] U.S. CONST. amend IV.

[10] *See* United States v. Jones, 565 U.S. 400, 404–405 (2012).

[11] Katz v. United States, 389 U.S. 347 (1967).

[12] *Id.* at 348.

[13] *Id.* at 353.

recognize as legitimate, justifiable, or reasonable.[14] Unfortunately, the Court did not establish a single reasonableness standard which lower courts could apply.[15] As Professor Orin Kerr explains, "The Supreme Court has not and cannot adopt a single test for when an expectation [of privacy] is 'reasonable' because no one test effectively and consistently distinguishes the more troublesome police practices that require Fourth Amendment scrutiny from the less troublesome practices that do not."[16]

The murkiness of *Katz* led to the growth of aggressive policing emboldened and sustained by the forty-year War on Drugs.[17] While traffic stops are the most common interaction society has with law enforcement, many United States residents are unaware of the vast discretion police have and number of tactics officers employ to pull over cars, hoping to find drugs.[18] Fully aware that the Supreme Court holds little interest in regulating traffic stops or preventing racial profiling, cops exercise broad authority to pull over cars for almost any alleged traffic violation such as having tinted windows, having a broken taillight, crossing over a fog line, or some other

---

[14] *Id.* at 361 (Harlan, J., concurring). David Gray offers this critique of *Katz*:

> Rather than creating out of whole cloth a novel definition of 'search,' the justice should have forced their attention on the text and history of the Fourth Amendment . . . [this] would have preserved the Fourth Amendment's focus on collective interests and the grants of broad and unfettered discretion to search and seize, which threaten those collective interests.

GRAY, *supra* note 8, at 250.

[15] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, *in* THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE, *supra* note 8, at 74 [hereinafter Kerr, *Four Models of Fourth Amendment Protection*]. David Gray wants the Court to abandon the *Katz* reasonable expectation of privacy test and adopt a common-sense definition of "search." David Gray, *The Fourth Amendment Categorical Imperative*, 116 MICHIGAN L. REV. ONLINE 14, 15 (2017) ("The reasonable expectation of privacy test has granted government agents unfettered discretion to engage in a wide variety of search activities completely free of Fourth Amendment regulation.").

[16] Kerr, *Four Models of Fourth Amendment Protection*, *supra* note 15, at 505–506. *See also* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 222 (2017) ("Modern technology is effectively erasing the distinction so critical in *Katz*: between what we knowingly expose to the public and what we seek to keep private.").

[17] *See* JAMES FOREMAN, JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 20, 25 (2017) (explaining that the drug war began with Richard Nixon's 1971 declaration of taking "a new, all-out offensive" against hard drugs and noting the federal government's role escalating the War on Drugs during the crack cocaine epidemic of the 1980s).

[18] *See* Wayne R. LaFave, *The "Routine Traffic Stop" from Start to Finish: Too Much "Routine," Not Enough Fourth Amendment*, 102 MICH. L. REV. 1843, 1854 (2004) (noting "probable cause as to a minor traffic violation can be so easily come by that its existence provides no general assurance against arbitrary police action."); Lewis R. Katz, "*Lonesome Road": Driving Without the Fourth Amendment*, 36 SEATTLE U. L. REV. 1413, 1414 (2013) ("The protections of the Fourth Amendment on the streets and highways of America have been drastically curtailed.").

inventive pretext.[19] In his Pulitzer Prize-winning book *Locking Up Our Own: Crime and Punishment in Black America*, Professor James Foreman refers to pretextual traffic stops as an easy tool for police to stop drivers as they please, stating, "[i]f a car draws suspicion from the police, they can almost invariably find a way to stop it illegally especially if they follow it long enough,"[20] and follow up with an explanation of one of the "techniques" the police use to secure consent."[21] Because officers are well-trained in conflating requests for license and registration, it is no wonder that the technique often results in an arrest and search.[22]

---

[19] *See, e.g.*, Whren v. United States, 517 U.S. 806 (1996) (holding that a police officer's observation of a traffic violation serves as sufficient authority to pull over the motorist, and the officer's true motive for stopping the motorist is irrelevant). *See also* LaFave, *supra* note 18, at 1844 (citing the "war on drugs" as the motivation behind the renewed interest of the police in traffic enforcement). LaFave contends, "[T]he police have co-opted as a weapon to be used in the 'war on drugs,' police make stops for the most insignificant conduct…and courts uphold those tactics by broad interpretation of the definition of the traffic offenses involved." *Id.* at 1847. Some scholars assert that the Court should consider the racial realities of the real world and the possibility that race influenced the officer's attitude in the encounter. *E.g.*, THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE, *supra* note 8, at 161 ("For years, black and brown motorists have been stopped and pulled over at rates greatly and disproportionate to their presence in the community."); Devon W. Carbado, *From Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence*, 105 CALIF. L. REV. 125, 129 (2017) (asserting that the legalization of racial profiling enables police to violently engage and confront African Americans); David A. Harris, "*Driving while Black" and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops*, 87 J. CRIM. L. & CRIMINOLOGY 544 (1997) (arguing that the police use traffic codes "to stop a hugely disproportionate number of African-Americans and Hispanics"); Tracey Maclin, *"Black and Blue Encounters" Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?*, 26 VAL. U.L. REV. 243, 250 (1991) (discussing the racial dynamics of challenged police confrontations and suggesting that "the Court should consider the race of the person confronted by the police, and how that person's race might have influenced his attitude toward the encounter."); Andrew E. Taslitz, *Respect and the Fourth Amendment*, 99 J. CRIM. LAW & CRIMINOLOGY 15, 21 (2003) (criticizing the Court's endorsement of a colorblind search and seizure jurisprudence while acknowledging the disparate impact on racial minorities caused by a contraction of Fourth Amendment rights); Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 989 (1999) (theorizing that some enforcement officers consciously or unconsciously "act on the basis of racial bias in denominating behavior as 'suspicious.'").

[20] Foreman, *supra* note 17, at 198.

[21] *Id.* at 200.

[22] *See id.* at 198, 200. Applying Foreman's theory to a hypothetical illustrates how pretextual stops work in practice. A Deputy Sheriff pulled over an automobile driven on Georgia State Route 402 East after it changed lanes with a left blinker that "appeared" to be broken, and after a passenger allegedly threw a cigarette out the window. The deputy advised the driver of the reason for the stop and asked the driver to exit from the vehicle. The driver complied and stepped to the rear of the vehicle. When the deputy asked the driver if he had any guns or knives on him, the driver answered negatively. No weapons or contraband were found during the subsequent pat down. The driver then presented his valid driver's license and denied having any marijuana when the deputy asked how much marijuana he and the passenger had in his possession. Still, the deputy insisted that he had "something" in the vehicle because he could smell it. The deputy then told the driver

A few hypothetical examples of typical Fourth Amendment drug enforcement scenarios help to illustrate the lengths the police will go to pull drivers over. First, imagine the police staking out a suspect's house based on a hunch about drug dealing, and then pulling over the target's car for making a U-turn on a deserted corner without signaling. Afterwards, the police pat down the driver and discover marijuana. Similarly, the police could just as easily pull over a car for failing to have a license plate light, which then leads to a probable cause and inventory search of the car and the discovery of drugs and a pistol in a backpack.

Second, it is worth noting that in recent years, an ostensibly innocuous fog lane violation has become another excuse for police to pull cars over. As I explored in an earlier article, law enforcement officers across the country have been increasingly initiating traffic stops, alleging that drivers crossed onto a fog line in violation of a state ordinance prohibiting such conduct.[23] Although these laws were enacted for the purpose of public safety, the police are instead relying on statutes as an excuse to pull over cars which may have only momentarily crossed the fog line, having otherwise done nothing unlawful.[24] This affords police "tremendous leeway to conduct pretextual stops, unreasonably detain suspects, and unlawfully search vehicles."[25]

Third, an officer can even pull over a car based on a mistaken belief that a violation has occurred. In *Heien v. North Carolina*,[26] the Court held that reasonable suspicion, as required for a traffic stop or an investigatory stop, can rest on a reasonable mistake of law in stopping a vehicle for which one of the brake lights was working.[27] Not surprisingly, the *Heien* ruling glosses over its real-world application: its analysis is centered on a doctrinal analysis of mistake of law that obscures the realities of law enforcement practices, including the common practices of the police in finding any

---

that this was his last opportunity to confess about having any marijuana. The driver then successfully completed a series of roadside sobriety tests administered by the deputy. The officer then repeated the same question he asked before, to which the driver again answered in the negative. Unsatisfied with the responses, the deputy detained the driver and called for a backup officer with a drug-sniffing dog to arrive. Eventually, the deputies located drugs during their search of the vehicle. Assuming arguendo that there was a valid reason for the traffic stop, the original justification for the stop ended, however, at the time the computer check was completed, and the driver's identification was verified.

[23] *See* Harvey Gee, "*U Can't Touch This" Fog Line: The Improper Use of a Fog Line Violation as a Pretext for Initiating an Unlawful Fourth Amendment Search and Seizure*, 36 N. ILL. U.L. REV. 1, 2 (2015). A fog line is "the white line that demarcates the shoulder from the road." Riche v. Dir. of Revenue, 987 S.W. 331, 333 (Mo. 1999) (en banc).

[24] Gee, *supra* note 23, at 2.

[25] *Id.*

[26] Heien v. North Carolina, 135 S. Ct. 530 (2014).

[27] *Id.* at 540.

excuse to follow and pull drivers over for alleged traffic violations, detecting "suspicious behavior" during small talk between the officer and driver about seemingly innocuous things such as vehicle registration and driving destination. However, Justice Sotomayor recognized this potential opportunity for police misconduct and expressed the dangers that could result in her dissent. Sotomayor highlighted the deference given to officers who evaluate, often quickly, the significance of facts out in the field[28] and underscored the fundamental unfairness in holding that a reasonable mistake of law can justify a Fourth Amendment seizure.[29] She further argued this would result in too many stops, resulting in constitutional violations because innocent citizens would be made to shoulder the burden.[30]

What can be done to curb such overreaching by the police? Perhaps with more information educating the general public, along with organized protests, activism, and legislative change, the almost arbitrary stopping of cars by law enforcement can be reduced. It is worthwhile to recall that it was this same kind of public outrage which led to public awareness about the practice of racial profiling.[31]

---

[28] *Id.* at 543 (Sotomayor, J., dissenting).

[29] *Id.* at 545 (Sotomayor, J., dissenting).

[30] *Id.* at 544 (Sotomayor, J., dissenting).

[31] After the Court's highly-criticized ruling allowing a traffic violation to serve as sufficient authority to pull over a motorist, regardless of the officer's motive, in Whren v. United States, 517 U.S. 806, 813 (1996), there was a manifestation in public outrage leading to regulation and legislation. *See* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: CASES AND COMMENTARY 333 (9th ed. 2007); Gabriel J. Chin & Charles J. Vernon, *Reasonable but Unconstitutional: Racial Profiling and the Radical Objectivity of* Whren v. United States, 83 GEO. WASH. L. REV. 882, 886 (2015). As Professor Foreman explains, "[p]retext[ual] stops are responsible for most of the racial disparity in traffic stops nationwide." FOREMAN, *supra* note 17, AT 212; Illya Lichtenberg, *Police Discretion and Traffic Enforcement: A Government of Men?*, 50 CLEV. ST. L. REV. 425, 426 ("Police across the nation have long been accused of using the broad discretion afforded to them in traffic enforcement as a pretext for criminal investigation."). Officers engage in racial profiling because pretextual stops allows them to pull over African Americans and other minority drivers more frequently than white drivers, as opposed to when officers are actually enforcing traffic laws. *See* FOREMAN, *supra* note 17, at 212, 214. *See also* Devon W. Carbado, *supra* note 19, at 130 (noting that after the effective legalization of racial profiling in *Whren*, "African Americans . . . experience the Fourth Amendment as a system of surveillance, social control, and violence, not as a constitutional boundary that protects them from unreasonable searches and seizures."). *But see* Paul Butler, *The System Is Working the Way It Is Supposed to: The Limits of Criminal Justice Reform*, 104 GEO. L.J. 1419, 126 (2016) [hereinafter Butler, *The System Is Working the Way It Is Supposed to*] (arguing that police practice of stopping and frisking African Americans and Latinos, and imposition of violence on them that results, operates as a legal and integral feature of a designed policing and punishment regime in the United States).

II. BEYOND *TERRY V. OHIO*: FROM ONE-ON-ONE ENCOUNTERS TO PROACTIVE LARGE-SCALE STOP AND FRISKS ON THE STREETS WITHIN A POLICE STATE

This Part examines the manner in which law enforcement exploits stop and frisks to create an occupied police state. A police officer may stop and frisk individuals and conduct routine, warrantless searches and seizures under the guise of "reasonableness" under *Terry v. Ohio*,[32] the landmark decision following *Katz*.[33] *Terry* involved suspects casing a jewelry store. Although officers lacked a warrant, they had reasonable and articulable suspicion for the stop which occurred during a crime in progress.[34] A gun was found on petitioner during a frisk.[35] Under *Terry*, officers must point to some objective facts or observations that are sufficient to show reasonable suspicion in the circumstance; courts then assess the reasonableness of searches and seizures from an objective point of view.[36] After *Terry*, it became increasingly unclear when stops were permissible.[37] Ironically, since 1968, the ruling has been used to support the use of proactive stop and frisks by police with almost impunity. But this practice of wholesale stop and frisks has proven to be only minimally effective in reducing crime.[38]

For the most part, *Terry* stops are disastrous for defendants. The police can justify their decision to stop and frisk regardless of the true motivation, and courts tend to give them the benefit of the doubt.[39] This almost never bodes well for the person searched. In fact, it presents a double-edged problem: (1) a person has no recourse if they are not arrested; and (2) if a person is arrested and charged, that person's suppression motion will likely be denied, given the great deference paid to an officer's justification for

---

[32] Terry v. Ohio, 392 U.S. 1, 24 (1968).

[33] Katz v. United States, 389 U.S. 347 (1967).

[34] *Terry*, 392 U.S. at 6–7.

[35] *Id.* at 7.

[36] SALTZBURG & CAPRA, *supra* note 31, at 42–43. ("[T]he [*Terry*] Court not only permitted stops and frisks on less than probable cause, it also explicitly invoked the reasonableness clause over the warrant clause as the governing standard.").

[37] *Cf.* FRIEDMAN, *supra* note 16, at 154.

[38] *See* GRAY, *supra* note 8, at 279, 281. Gray contends routine stop and frisks are constitutionally ineffective and "wholly contrary to the imperative command at the heart of the Fourth Amendment." *See also* FRIEDMAN, *supra* note 16, at 149 ("Warren's *Terry* opinion contained the seeds of enormous discretion for law enforcement . . . in the years to come."); Paul Butler, *Stop and Frisk and Torture-Lite: Police Terror of Minority Communities*, 12 OHIO ST. J. CRIM. L. 57, 57 (2014) [hereinafter Butler, *Stop and Frisk and Torture-Lite*] ("Because the 'reasonable suspicion' standard . . . is lenient, the police have wide discretion in who they detain and frisk. Even suspicion of a trivial offense like jaywalking, or spitting on the sidewalk, can give the police the authority to stop you.").

[39] *See* GRAY, *supra* note 8, at 279.

stopping and frisking, along with the officer's explanation for what constituted articulable suspicion for the stop.[40] Gray succinctly frames the issue, asserting that "leaving the power to conduct stops and frisks to the unfettered discretion of law enforcement would threaten the right of the people to be secure against unreasonable searches and seizures."[41]

Taking a broader analysis by considering the racial component, Professor Paul Butler argues that the Court's interpretation of the Constitution has largely failed to extend African American citizens protection from police abuse and sentencing disparities, and theorizes that the Court has given police unprecedented "super powers" to preserve the racial order in this country though the use of deadly force, arrest powers, and racial profiling.[42] Under this schema, he bluntly extols, "[T]he court is just reflecting the will of the (white) majority. Many people are afraid of African American men, and the Court has authorized police procedures to contain the perceived threat."[43]

---

[40] FRIEDMAN, *supra* note 16, at 154–56.

[41] GRAY, supra note 8, at 251. *See also* Butler, *Stop and Frisk and Torture-Lite*, *supra* note 38, at 57 ("Stops and frisk is, in the United States, a central site of inequality, discrimination, and abuse of power."). Friedman wants better police accountability because the police lack clear guidance about the legality of their activities and judges cannot be relied upon to regulate police actions, amounting to what Friedman calls policing without permission, an illegitimate practice. FRIEDMAN, *supra* note 16, at 16. *See also* Stephen J. Schulhofer et al., *American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative*, 100 J. CRIM. L. & CRIMINOLOGY 335, 374 (2011) (emphasizing the need to reconsider American policing styles and recommending "styles that communicate respect and nurture public trust" that benefit minority and majority communities alike).

[42] PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN 56–57 (2017).

[43] *Id.* at 57. Professor Butler decries Terry stop and frisks as "violent and destabilizing," and argues:

> For African Americans men, stop and frisk is a form of government. It is the most visceral manifestation of the state in their lives . . . virtually every African American man gets stopped-and-frisked. . . . It is the nation's leading crime control policy—despite scant evidence that it actually works to make communities safer.

Id. at . Relatedly, Professor Michelle Alexander, whose seminal work propelled the term "mass incarceration" into the vernacular, argues:

> The extraordinary racial disparities in our criminal-justice system would not exist today but for the complicity of the United States Supreme Court. In the failed war on drugs, our Fourth Amendment protections against unreasonable searches and seizures have been eviscerated. Stop-and-frisk operations in our communities are now routine; the arbitrary and discriminatory police practices the framers aimed to prevent are now commonplace.

Michelle Alexander, *The New Jim Crow*, AM. PROSPECT (Dec. 6, 2010), https://prospect.org/article/new-jim-crow-0. Mass incarceration is one part of a racially discriminatory criminal justice system. Drugs and the lengthy sentences meted out to non-violent offenders for having small amounts of drugs contributed to the mass incarceration of racial minorities in this country. *See* Devon W. Carbado, *Blue-on-Black Violence: A Provisional Model*

These academic concerns are supported by reality. Case in point, one of the most recent and visible examples of racially discriminatory stop and frisk policies was the New York City Police Department's proactive stop-and-frisk program which, until recently, mostly targeted African Americans. Even though a federal judge found the program to be unconstitutional, and there have been fewer stops, the racial profiling of African Americans and Latinos and aggressive policing continue in minority communities across the country.[44] Consider the U.S. Department of Justice ("DOJ")'s investigation of the Baltimore Police Department that came in the wake of the 2015 death of Freddie Gray, which found that the department engaged in a pattern or practice of violating the constitutional rights of community members, especially African Americans.[45] More specifically, the DOJ, led by then-Attorney General Eric Holder, reported that African Americans were subjected to "disproportionate rates of stops, searches and arrests; [used] excessive force; and [retaliated] against individuals for their constitutionally-protected expression."[46] But hopes for

---

of Some of the Causes, 104 GEO. L.J. 1479, 1485 (2016) (listing factors which render African Americans vulnerable to repeated police interactions, including policing practices, mass criminalization, racial stereotyping, and racial segregation); Paul Butler, *The System is Working the Way It Is Supposed to*, *supra* note 31, at 1423–25 (2016) (describing the racial injustices articulated by the movement for Black Lives). Having these systematic racial biases in mind, San Francisco Public Defender Jeff Adachi discussed the state of public defense in California and the United States and criminal justice reform including the need to reform bail, sentencing laws, and eliminate racial disparities, and offered a blueprint for racial justice calling for the formation of in-house racial justice communities, regional racial justice groups, implicit or unconscious bias training, community bridge building, overrepresentation of racial minorities in San Francisco's criminal justice system, litigating racial justice issues in jury selection and voir dire, bail charging and selective prosecution, racial profiling, and sentencing. *See generally* JEFF ADACHI ET AL., BLUEPRINT FOR RACIAL JUSTICE, https://sflawlibrary.org/sites/default/files/Racial%20Justice%20Blueprint_1.pdf (last visited Apr. 26, 2019). A similar position is espoused by David Gray, who argues urges that stop and frisk programs are ineffective and disproportionately target politically and economically vulnerable communities of color. *See* GRAY, *supra* note 8, at 276 ("Residents in urban areas, members of minority groups, and those who exhibit the markers of poverty are particularly likely to be stopped and frisked. . . . For many innocent, law-abiding residents in these communities the threat of being stopped or frisked is a matter of everyday routine.").

[44] *See* Jenn Rolnick Borchetta et al., *Don't Wreck Stop-and-Frisk Reforms*, N.Y. TIMES, Apr. 10, 2018, at A27 (analyzing the court-ordered reform process for the New York City Police Department to improve police discipline and supervision, and criticizing potential opposition towards police needed reforms while advocating three reforms: serious penalties for police misconduct; use of smart phones; and the creation of a city-wide community oversight board).

[45] U.S. DEP'T OF JUSTICE, CIVIL RIGHTS DIV., INVESTIGATION OF THE BALTIMORE POLICE DEPARTMENT 21 (2016), https://www.justice.gov/opa/file/883366/download.

[46] Press Release, Dep't of Justice, Office of Pub. Affairs, Justice Department Announces Findings of Investigation into Baltimore Police Department (Aug. 10, 2016), https://www.justice.gov/opa/pr/justice-department-announces-findings-investigation-baltimore-police-department. *See also* Steve Chapman, *Unreasonable Searches are Unconstitutional—and Common*, CHI. TRIB. (Aug. 15, 2016, 12:01 PM),

meaningful reform were dashed when the Trump administration's DOJ, first led by then-Attorney General Jeff Sessions, shifted away from oversight of police misconduct in Baltimore to stronger policing strategies focused on "maintaining law and civil order" that disproportionately impact the African American community.[47]

III. DIGITAL UPGRADE: SURVEILLANCE STATE TECHNOLOGY AND REFRAMING THE SUPREME COURT'S FOURTH AMENDMENT JURISPRUDENCE

This Part examines the Court's Fourth Amendment jurisprudence on the surveillance technology leading up to *Carpenter*: a decision which provides much needed protections against technologically-enhanced police surveillance powers.

---

https://www.chicagotribune.com/news/opinion/chapman/ct-fourth-amendment-baltimore-police-searches-unconstitutional-perspec-20160812-column.html.

[47] *See* James Braxton Peterson, *Jeff Sessions is Slowly but Surely Undoing America's Criminal Justice Progress*, NBC NEWS, https://www.nbcnews.com/think/opinion/jeff-sessions-slowly-surely-undoing-america-s-criminal-justice-progress-ncna823126 (last updated Nov. 23, 2017, 1:22 AM). *See also, e.g.*, Lois Beckett, *How Jeff Sessions and Donald Trump Have Restarted the War on Drugs*, GUARDIAN (Aug. 21, 2017, 2:00 PM), https://www.theguardian.com/us-news/2017/aug/21/donald-trump-jeff-sessions-war-on-drugs; Matt Ford, *A Chance for Criminal Justice Reform Under Trump*, NEW REPUBLIC (Feb. 5, 2018), https://newrepublic.com/article/146940/chance-criminal-justice-reform-trump; Laura Jarrett & Eugene Scott, *AG Sessions Paves Way for Stricter Sentencing in Criminal Cases*, CNN, https://www.cnn.com/2017/05/12/politics/sessions-criminal-charging-memo/index.html (last updated May 12, 2017, 11:55 AM); Vann R. Newkirk II, *The People Trump's War on Drugs Will Actually Punish*, ATLANTIC (Mar. 26, 2018), https://www.theatlantic.com/politics/archive/2018/03/killing-drug-dealers-opioid-epidemic/555782/; Udi Ofer, *ACLU Poll Finds Americans Reject Trump's Tough-On-Crime Approach*, AM. C.L. UNION (Nov. 16, 2017, 1:45 PM), https://www.aclu.org/blog/smart-justice/aclu-poll-finds-americans-reject-trumps-tough-crime-approach. Attorney General Jeff Sessions did not actively investigate systematic policing abuses. Sessions adopted a tough-on-crime approach echoing the war on drugs by authorizing federal prosecutors to prosecute marijuana sellers and calling for mandatory minimum sentences for sellers of smaller amounts of drugs, even in states where marijuana was legalized, charging suspects with the most serious offense available. *See* German Lopez, *Jeff Sessions Turned Trump's "Tough on Crime" Dreams into a Reality*, VOX (Nov. 7, 2018, 4:50 PM), https://www.vox.com/policy-and-politics/2018/11/7/18073074/jeff-sessions-resigns-war-on-drugs- crime. All of this coincided with the DOJ's dramatic shift from its historic mission of enforcing civil rights protections of African Americans and other racial minorities, immigrants, and LGBT people—to protecting people of faith, supporting state restrictive voting laws, and reducing oversight of police departments. *See* Katie Benner, *Trump's Justice Department Redefines Whose Civil Rights to Protect*, N.Y. TIMES (Sept. 3, 2018), https://www.nytimes.com/2018/09/03/us/politics/civil-rights-justice-department.html; Anya Kamentz, *Here's What's Going on With Affirmative Action and School Admissions*, NPR (July 7, 2018, 6:00 AM), https://www.npr.org/sections/ed/2018/07/07/626500660/everything-that-s-going-on-with-race-ethnicity-and-school-admissions-right-now.

Undoubtedly, proactive policing accelerated further after the September 11th attacks on the World Trade Center and the Pentagon: interbranch cooperation connected ordinary policing with fighting terrorism, facilitating unjustified intrusions onto civil liberties and personal privacy in the twenty-first century.[48] Federal agencies can gather meta data associated with domestic phone calls and private server networks and capture user content and communications from personal online activities under the auspices of the USA Patriot Act, which authorizes the federal government to issue warrantless searches and seizures and intercept electronic communications, including wiretaps.[49] Nearly eighteen years later, new technologies have only expanded this enormous power. Data technologies, algorithms, facial recognition, social media scraping, data mining, person-based and place-based predictive analytics that correlate with criminal activity, and reliance on "big data" are driving police investigations and surveillance today.[50]

As with the earlier discussion regarding traffic stops in Part I, concrete examples help to illustrate just how far law enforcement will go in using new technology to circumvent the Fourth Amendment. One commonly used tool is the ShotSpotter, a strategically placed network of powerful acoustic sensors connected to the Global Positioning System ("GPS").[51] ShotSpotters automatically identifies the sounds of gunshots and pinpoints an exact location to alert police to potential violent crime before it is reported by human witnesses.[52] These devices have been deployed in over 90 cities,[53] including Washington, D.C., Boston, Oakland, San Francisco,

---

[48] *See* FRIEDMAN, *supra* note 16, at 14.

[49] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272. *See also* ANGELA J. DAVIS, ARBITRARY JUSTICE: THE POWER OF THE AMERICAN PROSECUTOR 115 (2007); THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND CONTEMPORARY DEBATE, *supra* note 10, at 262.

[50] ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 2, 4, 167 (2017). *See also* Andrew G. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 125 (2002) (describing the use of facial recognition technology by Florida police to survey a downtown nightlife district); Natasha Singer, *Facebook Pores Over Its Prize Asset: Faces*, N.Y. TIMES, July 10, 2018, at B1; Robyn Greene, *How Cities Are Reining in Out-of-Control Policing Tech*, SLATE (May 14, 2018 1:58 PM), https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html.

[51] *How ShotSpotter Works*, SHOTSPOTTER, https://www.shotspotter.com/ (last visited Apr. 27, 2019); Chris Weller, *There's a Secret Technology in 90 U.S. Cities that Listens for Gunfire 24/7*, BUS. INSIDER (June 27, 2017, 10:59 AM), https://www.businessinsider.com/how-shotspotter-works-microphones-detecting-gunshots-2017-6.

[52] Weller, *supra* note 51.

[53] *Id.*

and Minneapolis.[54] ShotSpotter sensors can also pick up outside conversions, sounds, and other audio without the consent and knowledge of individuals and which could be used in the prosecution's case against a criminal defendant.[55]

Understandably, this reliance on emerging technologies by law enforcement spurred debates over their invasiveness, and concerns about personal privacy and law enforcement's circumvention of the warrant requirement continues to grow. The threat to personal privacy is real. In fact, the U.S. District Court for the District of Columbia released information showing a sevenfold surge in law enforcement requests to track Americans without warrants through cell phone locations and internet activity in the past three years.[56] All told, these technological tools that assist police investigations are testing the boundaries of the Fourth Amendment, as this enhanced ability of law enforcement to spy on citizens poses an enormous threat to liberty and free expression.[57] Their use begs the Court's Fourth Amendment jurisprudence to be tweaked further so that privacy issues posed by new technology can be adequately addressed.[58]

---

[54] FERGUSON, *supra* note 50, at 88.

[55] Suraj K. Sazawal, *Is ShotSpotter Violating Your Fourth Amendment Rights and You Don't Even Know?*, DISSENT NEWSWIRE (May 8, 2015), https://rightsanddissent.org/news/is-shotspotter-violating-your-fourth-amendment-rights-and-you-dont-even-know/. *See also* Alexandra S. Gecas, Note, *Gunfire Game Changer or Big Brother's Hidden Ears?: Fourth Amendment and Admissibility Quandaries Relating to Shotspotter Technology*, 2016 U. ILL. L. REV. 1073, 1077, 1107 (2016) (discussing the Fourth Amendment implications posed by ShotSpotters' ability to record conversations). In aiming towards a goal of more transparency, government agencies should release information that contributes to the public's awareness and conversation about the efficacy of ShotSpotters, so the public has the opportunity to learn about the reliability of ShotSpotters, the retention period for the data collected, and whether the data is shared.

[56] Spencer S. Hsu, *In District, Warrantless Tracking Requests Surge in Past 3 Years*, WASH. POST, July 19, 2017, at B1. Equally concerning are reports of foreign spies who are using StingRays in Washington, D.C. to track and intercept calls. *See* Veronica Stracqualsuri, *Senators Demand More Information About DC Mobile Snooping Devices*, CNN, https://www.cnn.com/2018/04/18/politics/senators-dhs-stingrays-washington-dc/index.html (last updated Apr. 18, 2018, 12:39 PM).

[57] FRIEDMAN, *supra* note 16, at 9.

[58] *See* MICHAEL C. GIZZI & CRAIG CURTIS, THE FOURTH AMENDMENT IN FLUX: THE ROBERTS COURT, CRIME, CONTROL, AND DIGITAL PRIVACY 76 (2016) (describing cases in which the Court reconceptualized Fourth Amendment protections); GRAY, *supra* note 8, at 225 (underscoring the need for the Court, relying on the Fourth Amendment, to fashion new Fourth Amendment remedies to twenty-first century technologies.); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 383 (2004) [hereinafter Kerr, *The Fourth Amendment and New Technologies*] (questioning the continuing vitality of *Katz* in an era where the public's reliance on cell phones for private communication have supplanted public telephones and highlighting the complexities created by technological change for the purpose of Fourth Amendment analysis). Kerr explains, "Because the Fourth Amendment applies only to actual searches, not the technologies that merely have the potential to

A. *CARPENTER V. UNITED STATES*: POSITIONING A RESILIENT FOURTH AMENDMENT ON A PRO-PRIVACY TRAJECTORY IN THE DIGITAL AGE

Carpenter v. United States[59] is one of the most important privacy decisions in the digital age. *Carpenter* held that "individuals have a reasonable expectation of privacy in the whole of their physical movements."[60] In doing so, the Court reframed the third-party doctrine[61] by expanding the Fourth Amendment to cover all other digital technologies that also implicate locational privacy in public.[62] But the ruling was narrow in its scope and is not applicable to obtaining cell-site location records in real time, getting information about all of the phones that connected to a particular tower at a specific time, national security, or an "urgent situation."[63]

The case involved Timothy Carpenter, who organized bands of robbers that held up nine Radio Shack and T-Mobile cell phone stores in Michigan and Ohio. Carpenter was apprehended after one of the suspects gave police the names and cell phone numbers of Carpenter and his fifteen accomplices.[64] Relying on the Stored Communications Act, which required a showing that the data was "relevant and material" to the ongoing investigations, prosecutors obtained subpoenas from a federal magistrate judge to secure records of Carpenter's general location information from his

---

conduct searches, counts generally cannot pass on how the Fourth Amendment applies to a technology until long after a technology has been introduced." *Id.* at 868.

[59] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[60] *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012)).

[61] The third-party doctrine, established by United States v. Miller, 425 U.S. 435 (1976) and Smith v. Maryland, 442 U.S. 735 (1979) refers to when information is in the hands of third parties; an individual can have no reasonable expectation of privacy in that information, making the Fourth Amendment inapplicable. *Miller*, 425 U.S. at 443.

[62] *Carpenter*, 138 S. Ct. at 2219–20.

[63] *Id.* at 2220–21; Amy Howe, *Opinion Analysis: Court Holds That Police Will Generally Need a Warrant for Sustained Cellphone Location Information*, SCOTUSBLOG (June 22, 2018, 6:01 PM), http://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/. *See also* Adam Liptak, *Warrant Required for Cellphone Tracking Data*, N.Y. TIMES, June 23, 2018, at A1; Jake Laperuque, *The* Carpenter *Decision: A Huge Step Forward for Privacy Rights but Major Problems Remain*, POGO (June 28, 2018), http://www.pogo.org/blog/2018/06/the-carpenter-decision-a-huge-step-forward-for-privacy-rights-but-major-problems-remain.html ("The Court explicitly declared that it was providing a narrow ruling that only applied to a government demand for cellphone location data from the past, and was not taking on the question of whether ongoing location surveillance in real-time should require a warrant as well."); Eunice Park, *Protecting the Fourth Amendment After* Carpenter *in the Digital Age: What Gadget Next?*, ORANGE COUNTY LAW. MAG., May 21, 2018, at 35 (discussing the applicability of the then-forthcoming ruling in *Carpenter* and anticipating the repercussions for lower courts addressing future Fourth Amendment technology-based challenges such as StingRay and other technologies coming up on the horizon).

[64] *Carpenter*, 138 S. Ct. at 2212.

cell phone provider, for the purpose of connecting his whereabouts over a four-month period with the dates, times, and locations of the robberies.[65] The government offered as evidence Carpenter's cell phone records from his wireless carriers; its collection of 127 days of Carpenter's cell-site locator information ("CSLI") placed Carpenter within a half-mile to two miles of scenes of the robberies.[66] At trial, Carpenter unsuccessfully argued that the government's collection of these records constituted a warrantless search in violation of the Fourth Amendment, and the CSLI was key in securing his conviction.[67]

Chief Justice Roberts, writing for a five-justice majority,[68] ruled that cell phone users possess a reasonable expectation of privacy in the CSLI history associated with their cell phones.[69] Accessing a person's historical cell-site records—or at least seven days or more of cell-site records—is a Fourth Amendment search because it violates the person's "legitimate expectation of privacy in the records of his physical movements."[70] The majority further held that law enforcement agencies generally need a warrant to track suspects' locations using CSLI.[71]

Carpenter is a natural extension of the line of reasoning introduced in three earlier decisions substantively ruling against government surveillance: *Kyllo v. United S*tates,[72] *United States v. Jones*,[73] and *Riley v. California*.[74] First, in *Kyllo*, the Court held that the use of a thermal imaging device that is not in general public use, aimed at a private home from a public street to detect relative amounts of heat and obtain information about the interior of a home, constituted a "search" under the Fourth Amendment.[75] Justice Scalia, writing for the Court, acknowledged that the advance of technology affects the degree of privacy secured by the Fourth Amendment, and police technology would erode such privacy, absent such protections.[76] After

---

[65] *Id.*

[66] *Id.*

[67] *Id.* at 2212–13.

[68] Chief Justice Roberts was joined by Justices Breyer, Ginsburg, Kagan, and Sotomayor.

[69] *Carpenter*, 138 S. Ct. at 2217.

[70] *Id.*

[71] *Id.* at 2222.

[72] Kyllo v. United States, 533 U.S. 27 (2001).

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

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

[75] *Kyllo*, 533 U.S. at 40. *See also* Taslitz, *supra* note 50, at 133 ("The Supreme Court has generally failed to see any enhanced dangers to privacy caused by rapidly changing police surveillance technologies. Instead, the Court has addressed technology questions under the same analytical framework that it uses for resolving all Fourth Amendment search questions. This framework is one that privileges the home over at the expense of other venues.").

[76] *Kyllo*, 533 U.S. at 33–34.

Kyllo, the question remained: does electronic tracking surveillance outside the home constitute a search under the Fourth Amendment?[77]

Second, in *United States v. Jones*, a unanimous Court expressed discomfort with the government's attachment of a GPS tracker on a car over 28 days, which was determined to be a "search."[78] Instead of addressing the issue of the application of the *Katz* test head on, the majority sidestepped and used common-law trespass theory.[79] A "search" under the trespass theory occurs when the government purposefully attempts to find something or obtain information by physically intruding on a constitutionally protected area, and a "seizure" occurs when there is some meaningful interference with an individual's possessory interests in that property.[80] Scalia wrote, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[81] In contrast, Justices Ginsburg, Breyer, Alito, Sotomayor, and Kagan, in a separate concurrence, expressed overarching concerns about the impact of contemporary surveillance technologies on Fourth Amendment rights.[82]

Notably, Sotomayor wrote a separate influential concurrence later relied upon by the *Carpenter* majority, in which she explained why the Court's Fourth Amendment search and seizure doctrine has become "ill suited [sic] to the digital age."[83] Among her key points, she stated that "[t]he government's physical intrusion on Jones's Jeep, erodes . . . longstanding protection for privacy expectation inherent in items of property that people possess or control."[84] Sotomayor cautioned about the government's ability of monitoring through GPS-enabled smartphones. She expressed that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and recognized the

---

[77] *See* Adam Liptak, *How a Radio Shack Robbery Could Spur a New Era in Digital Privacy*, N.Y. TIMES (Nov. 27, 2017), www.nytimes.com/2017-11-27.us.politics.supreme-court-fourth-amendment-privacy-cellphones.html.

[78] *See* United States v. Jones, 565 U.S. 400, 403–408 (2012).

[79] *See* FRIEDMAN, *supra* note 16, at 225. (asserting that *Jones* provides little guidance as to what kinds of location tracking or technology constitutes a search because the Court declined to modify its Fourth Amendment doctrine, instead deeming the tracking in *Jones* a search because the government had "physically occupied private property for the purpose of obtaining information." (quoting *Jones*, 565 U.S. at 404)).

[80] *Jones*, 565 U.S. at 406–407.

[81] *Id.* at 409 (emphasis in original).

[82] Justice Alito voiced concern over long-term surveillance and articulated, "the best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case and involved a degree of deprivation of privacy that a reasonable person would not have anticipated." *Id.* at 430 (Alito, J., concurring).

[83] *Id.* at 417 (Sotomayor, J., concurring).

[84] *Id.* at 414 (Sotomayor, J., concurring).

consequential chilling effect.[85] As for the public's reasonable societal expectation of privacy, Sotomayor doubted that people would be willing to exchange their expectations of privacy for more convenience or find the warrantless disclosures of their tracked public movements to be acceptable.[86] Foreshadowing the future, Sotomayor questioned the viability of the third-party doctrine established by *United States v. Miller*[87] and *Smith v. Maryland*[88]: when information is in the hands of third parties, an individual can have no reasonable expectation of privacy in that information, making the Fourth Amendment inapplicable.[89] It is the third-party doctrine that allowed the government to win the vast majority of the courtroom battles over the use of CSLI in criminal prosecutions before *Carpenter*.[90]

---

[85] *Id.* at 415 (Sotomayor, J., concurring).

[86] *Id.* at 417–18 (Sotomayor, J., concurring).

[87] United States v. Miller, 425 U.S. 435 (1976). In *Miller*, federal agents presented subpoenas to two banks to produce financial records of the defendant. *Id.* at 438. The Court held that this did not violate the Fourth Amendment because there was no reasonable expectation of privacy in financial records voluntarily conveyed to and regularly maintained in the ordinary course of business by a bank, such as financial statements and deposit slips. *Id.* at 442.

[88] Smith v. Maryland, 442 U.S. 735 (1979). In *Smith*, police officers had a pen register, which records the numbers dialed on an individual telephone line, installed at a robbery suspect's home. *Id.* at 737. The Court concluded that a telephone user had no reasonable expectation of privacy in information gathered from a pen register, distinguishing it from the listening device in *Katz* that "acquire[d] the *contents* of communications." *Id.* at 741 (emphasis in original).

[89] *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). *See also* GRAY, *supra* note 8, at 84; STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 132 (2012). The Fourth Amendment safeguards should apply whenever citizens convey personal information to a third party under promise of confidentiality. The courts should restore the Fourth Amendment "to its intended position as a mechanism for preserving those spaces in the fact of unprecedented technological, social, and political pressures." SCHULHOFER, *supra*, at 143.

[90] There have been multiple splits on the issue of whether a warrant is required by law enforcement agencies to collect cell phone information. Several state courts recognize a privacy interest in long-term tracking. *E.g.*, Commonwealth v. Rousseau, 990 N.E.2d 543, 553 (Mass. 2013); People v. Weaver, 990 N.E.2d 1195, 1202 (N.Y. 2009). A minority of courts focus on privacy and conclude that the third-party doctrine should not apply to historical CSLI because it reveals information about people and their things inside homes and other private spaces—expectation of privacy is at its pinnacle. These courts have relied on similar legal analyses to reach their conclusions. Massachusetts, New Jersey, Florida and the Northern District of California recognize a privacy interest in CSLI, and these courts require the government to get a warrant. *E.g.*, State v. Earls, 70 A.3d 630, 642, 644 (N.J. 2013) (holding that cell phone users have a reasonable expectation of privacy in their cell phone location information, and that police must obtain a search warrant before accessing that information); Tracey v. State, 152 So. 3d 504, 525 (Fla. 2014) (addressing the issue of whether the warrantless use of electronically-generated CSLI to track an individual's movements, in real time both on public roads and into a residence violates a subjective expectation of a privacy in that person's location, and holding that a subjective expectation of privacy of location as signaled by one's cell phone—even on public roads—is a reasonable expectation of privacy that society is now prepared to recognize). *See also In re* Tel. Info. Needed

Third, in *Riley v. California*, the Court addressed whether an officer's search of a defendant's smart phone incident to an arrest violated the Fourth Amendment and ruled unanimously that police generally must obtain a warrant to search the contents of cell phones.[91] *Riley* recognized the privacy interests in the kinds of vast data stored in modern cell phones which are persuasive today.[92]

These important decisions set the stage for *Carpenter* where in acknowledging the "seismic shifts in digital technology," Roberts raised concerns about the current and future potential for abuse if the government can collect a week or more of a person's data without having to show probable cause.[93] This is especially worrisome given the ubiquity of cellphones. Roberts pointed out that tracking historical cell-site records is much more invasive than GPS monitoring, channeling Justice Sotomayor's concurrence in *Jones* and during oral argument in *Carpent*er:

> While individuals regularly leave their vehicles, they compulsively carry cell phones with them at all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices,

---

for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015) (holding that cell phone users have an expectation of privacy in the historical CSLI associated with their cell phones, and that society is prepared to recognize that expectation as objectively reasonable); People v. Gordon, 68 N.Y.S.3d 306, 308, 311 (N.Y. Sup. Ct. 2017) (holding that the government's reliance on New York's pen register statute is inapplicable to cell-site simulators and observing, "By its very nature . . . the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping, and requires a separate warrant supported by probable cause [rather than solely a pen register warrant]."). However, pre-*Carpenter*, the Fourth, Fifth, Sixth, and Eleventh Circuits held that no privacy interest exists, and people voluntarily disclose their location data. United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc) (holding that the government's acquisition of historical CSLI from the defendant's cell phone provider without a warrant did not violate the Fourth Amendment); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (addressing the constitutionality of whether court orders authorized by the Stored Communications Act to compel cell phone service providers to produce historical cell site information of their subscribers, and ruling that orders to obtain historical cell-site information for specified cell phones at the points at which the user places and terminated a call are not categorically unconstitutional); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2010), *rev'd*, 138 S. Ct. 2206 (2018); United States v. Davis, 785 F.3d 498 (11th Cir. 2011) (en banc). The Third Circuit did not require probable cause in obtaining a warrant for CSLI. *In re* United States for an Order Directing Provider of Elec. Commc'n Servs. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3rd Cir. 2010) (holding that to obtain an order compelling production of a customer's CSLI, the government had a lesser burden than establishing probable cause, but if the government made requisite showing on remand, the court had discretion to require a warrant prior to ordering a cell phone provider to produce customer's CSLI).

[91] Riley v. California, 573 U.S. 373, 401 (2014).

[92] *Id.* at 396. Cell phones contain information about internet searches, browsing history, and reveal enough personal information private interests in the aggregate to reconstruct a person's private life. *Id.*

[93] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

> political headquarters, and other potentially revealing locales. . . . [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.[94]

At the core of the majority opinion, Roberts stressed the need to keep in mind the intention of the Framers of the Constitution and avoid a purely "mechanical interpretation" of the Fourth Amendment.[95] Roberts referred to the voluminous amount of information secured by the government and compared those capabilities to the GPS monitoring in *Jones*, particularly noting the ability to chronicle a person's past movements through the record of cell phone signals:

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."[96]

Accepting this reality, the majority reframed the third-party doctrine by limiting and departing from a tradition of deference paid to the doctrine, and declining to extend *Smith* and *Miller* to cover CSLI location information.[97] Believing that privacy rights are diminished but not entirely eliminated under the doctrine, the majority emphatically rejected the government's argument that people lose their privacy rights when using

---

[94] *Id.* at 2218. *See also* Mark Joseph Stern, *Sotomayor, Fourth Amendment Visionary: How the Supreme Court Vindicated the Justice's Prescient Theory of Digital Privacy*, SLATE (June 24, 2018, 5:56 PM), http://slate.com/news-and-politics/2018/06/in-carpenter-v-united-states-the-supreme-court-vindicates-justice-sonia-sotomayors-theory-of-digital-privacy.html (discussing Roberts's reliance in *Carpenter* on Sotomayor's concurrence in *Jones*, as reflected in Roberts' repeated citations to Sotomayor's concurrence).

[95] *Id.* at 2214.

[96] *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Scholars have voiced similar concerns. *See, e.g.*, Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1358–62 (2008) (warning that courts are overlooking the significant threat to liberty posed by technology such as GPS tracking bracelets, biometric scanners, and sex offender and DNA database indexes).

[97] *Carpenter*, 138 S. Ct. at 2212. *See also* Kerr, *Understanding* Carpenter, *supra* note 6; Editorial Board, *Congress Must Reckon with the Fourth Amendment and New Technology*, WASH. POST (June 23, 2018), www.washingtonpost.com/amphtml/opinions/congress-must-reckon-with-the-fourth-amemdment-and-new-technology/2018/06/23/195578cO-7653-11c8-9780-bldd6a09b549_story_html ("The *Carpenter* decision reflects a broader shift in the way the court interprets the Fourth Amendment, an interpretation that is gradually evolving to accommodate new technological realities.").

these technologies, intimating that the third-party doctrine is less of a bright-line rule and more of a fact-specific standard.[98]

Four dissenting justices separately voiced complaints and concerns.[99] The collective thrust of the dissents was embedded in Kennedy's argument that the third-party doctrine should control CSLI business records, and the government has a legal right to obtain them without a warrant.[100] Rejecting a broader view of privacy rights, Kennedy argued in favor of treating cell-site records like business records, claiming that Carpenter had no possessory interest in them[101] and, conversely, that the government has a lawful right to obtain by compulsory process.[102] Further, in contrast to Sotomayor's viewpoint in her *Jones* concurrence, Kennedy opined that Americans are aware of their lesser expectation of privacy in the digital age and voluntarily share their location with the public via social media.[103]

Lastly, *Carpenter* is far from being definitive. Major ramifications await for Fourth Amendment cases involving smart phones and information held by third-parties, including browsing data, text messages, emails, bank records, and personal records.[104] For instance, lower courts must grapple with *Carpenter*'s silence about: (1) whether the ruling can be applied retroactively to data collected prior to the *Carpenter* decision; (2) whether law enforcement can seek CSLI, without a warrant, for a period of less than seven days of cell-site data; and (3) the precise depth and scope of *Carpenter*-compliant searches.

---

[98] Kerr, *Understanding* Carpenter, *supra* note 6.

[99] The dissenting justices (apart from Justice Kennedy) offered divergent analytical approaches. First, Justice Alito argued that the majority's ruling violates the original understanding of the Fourth Amendment by giving defendants the right to object to the search of a third party's property. *Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting). Second, Justice Thomas offered the longstanding generic rejection of *Katz* and the reasonable expectation of privacy test, claiming that the Court eliminates the distinction between an individual's privacy and "a reasonable expectation of privacy in someone else's business records." *Id.* at 2236 (Thomas, J., dissenting). Third, Gorsuch was more concerned with the lack of guidance to the lower courts in his dissent, and suggested that they were "left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition." *Id.* at 2267 (Gorsuch, J., dissenting).

[100] *Id.* at 2223–24 (Kennedy, J., dissenting).

[101] *Id.* at 2228 (Kennedy, J., dissenting).

[102] *Id.* at 2224 (Kennedy, J., dissenting).

[103] *Id.* at 2232 (Kennedy, J., dissenting).

[104] *See* Laperuque, *supra* note 63 ("The Court explicitly declared that it was providing a narrow ruling that only applied to a government demand for cellphone location data from the past, and was not taking on the question of whether ongoing location surveillance in real-time should require a warrant as well.").

IV. PRIVACY AND THE FOURTH AMENDMENT AFTER *CARPENTER*: ARGUING AGAINST THE UNCONSTITUTIONAL USE OF STINGRAY SURVEILLANCE TECHNOLOGY

This section explains why the use of Stingray surveillance technology by the government poses a threat to our personal privacy, concluding that tracking a person's phone via Stingray technology constitutes a search, and as such, a warrant should be required for its use.[105] As Professor Susan Freiwald and Stephen Wm. Smith recently wrote in the *Harvard Law Review*:

> The case for Fourth Amendment protection of cell site simulator location data would seem *even stronger* than in *Carpenter*. The data gathered by the cell site simulator is *generated by law enforcement*, not the provider . . . Another problem with the cell site simulator is the breadth of the area under search. Allowing a police van to troll the streets of a neighborhood or town in order to locate a particular phone raises the specter of an illegal general warrant.[106]

---

[105] *See* Andrew Hemmer, Note, *Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches*, 91 CHI-KENT L. REV. 295, 297 (2016) (raising concerns that Stingrays may violate the Fourth Amendment). In the litigation over Stingrays' use, the government generally argues that there is no Fourth Amendment violation because (1) it is not getting information from the phone itself, since Stingray surveillance relies solely on tracking signals; (2) people know about the prevalence of available data from phone use, so no expectation of privacy exists; (3) no search warrant is needed because there is no reasonable expectation of privacy; and (4) phone communication information is held by a cell phone provider keeping phone information as a standard business record. The Seventh Circuit sided with the government's use of Stingrays in *United States v. Patrick*, 842 F.3d 540 (2016). when the panel majority punted on the substantive questions about whether a warrant was required to use the Stingray, and whether a cell-site simulator is a reasonable means of executing a warrant, and narrowly ruled that Patrick did not have any privacy interest in a public place, and reasoned that regardless of the Stingray, Patrick was taken into custody based on probable cause and an arrest warrant. *Id.* at 544. In making that determination, the panel majority paid deference to law enforcement's assurances that Stingrays are not invasive, and merely relied on the Department of Justice Policy Guidance manual's boilerplate disclaimer stating that cell-site simulators do not function as GPS location or capture emails texts, contact lists, images or other phone dates, or provide subscriber account information. *Id.* at 543. Pre-*Carpenter*, authority for the government's position was found in open registry case law and the stored communications act, both requiring a lower threshold of proof. *See* Pell & Soghoian, *supra* note 4, at 154–55 (relaying that the Department of Justice believes that Stingray surveillance is authorized by the Pen/Trap statute, which was enacted following *Smith v. Maryland* to aid law enforcement in using pen registers in its investigations). *But see* Owsley, *supra* note 4, at 186 (asserting that "cell site simulators are not pen registers and thus are not covered by pen register statute.").

[106] Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance* 132 HARV. L. REV. 205, 229 (2018) (emphasis added).

A. THE SECRET USE OF STINGRAY SURVEILLANCE TECHNOLOGY BY LAW ENFORCEMENT

While still celebrating the *Carpenter* ruling, privacy rights activists and defense attorneys remain committed to their almost decades long fight against the use of military grade cell-site simulators, best known as Stingrays and sometimes referred to as Triggerfish, IMSI Catchers, or Digital Analyzers. Originally developed for military and national security use,[107] a Stingray acts as a phony cell phone tower by sending powerful electronic signals to all cell phones within its two-block range to "trick cell phones in the area into transmitting their locations and identifying information."[108] Federal and local law enforcement use Stingrays—without a warrant—to secretly track individuals suspected of criminal activity, or to conduct mass surveillance on areas or groups of people.[109] Significantly, the general public is largely not aware of their use and misuse. Regrettably, the employment of Stingray technology has become commonplace.[110]

In the simplest terms, Stingrays resemble large metallic radio transmitters, and are the size of a suitcase and can be held by hand, placed in a car, or mounted on a drone or airplane. They capture texts, numbers of outgoing calls, emails, serial numbers, identification, GPS location, actual content of conversation, and other raw and detailed information from unsuspecting phones and track the location of targets and non-targets in apartments, cars, buses, and on streets though mapping software. They can even make the tracked device send texts and make calls.[111] There are also

---

[107] ADAM BATES, CATO INST., STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE 2 (2017), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa-809-revised.pdf.

[108] *Stingray Tracking Devices: Who's Got Them?*, AM. C.L. UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them (last updated Nov. 2018).

[109] *See, e.g.*, Alicia Lu, *What is StingRay, The Creepy Device Chicago Police: "Used to Spy" On Eric Garner Protesters?*, BUSTLE (Dec. 9, 2014) http://www.bustle.com/articles/53050-what-is-stingray-the -creepy-device-chicago-police-used-to-spy-on-eric-garner-protesters.

[110] *See* GRAY, *supra* note 8, at 5 ("Cell site simulators have become so common in the last ten years that it is virtually certain that everyone who has a cellular device has been subjected to surveillance by a cell site simulator.").

[111] *E.g.*, GRAY, *supra note* 9, at 4–5; Hemmer, *supra* note 105, at 295–96 (describing the tracking abilities of Stingrays and how they can "hijack[]" a phone to perform calls and texts disguised as the targeted phones); Austin McCullough, *StingRay Searches and the Fourth Amendment Implications of Modern Cellular Surveillance*, 53 AM. CRIM. L. REV. ONLINE 41, 41 (2016); Pell & Soghoian, *supra* note 2, at 145; Lu, *supra* note 109; Marian Hetherly, *Judge Rules Surveillance Info Collected by Police Stingrays Can Remain Confidential*, WBFO (Apr. 12, 2018), http://news.wbfo.org/post/judge-rules-surveillance-info-collected-police-stingrays-can-remain-confidential; Kim Zetter, *California Police Used Stingrays in Planes to Spy on Phones*, WIRED (Jan. 27, 2016, 6:28 PM), https://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/.

collateral consequences resulting from their use, including the disruption of cell service to phones in the form of service outages, blocked and dropped calls, and causing a connected cellphone's battery to drain and die.[112]

More precise then the CSLI tracking range of one eighth to four square miles at issue in *Carpenter*, Stingrays can identify the almost precise location of a person within six feet.[113] The use of Stingrays are also more nefarious than the collection of the CSLI history because unlike CSLI, warrantless cell phone tracking by Stingrays does no go through any third-party cell phone company carrier.[114] To be fair, there are legitimate uses of Stingrays. For example, Stingrays have proven to be useful in tracking down dangerous fugitives on crime sprees, including the suspect responsible for four Texas bombings earlier this year.[115] They are invaluable tools in intelligence gathering in terrorism cases when there is an immediate threat to human life, and other emergency situations.

Presently, Stingrays are used to track Americans through cell phone locations and internet activity by 13 federal agencies including the FBI, the DEA, the Department of Homeland Security ("DHS"), the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the NSA, Immigration and Customs Enforcement ("ICE"), and by police departments in over 25 states and the District of Columbia.[116]

The government's great enthusiasm for Stingrays is reflected by its willingness to pay the high cost—the units have a price tag between $16,000

---

[112] Brian Barrett, *The Baltimore PD's Race Bias Extends to High-Tech Spying, Too*, WIRED (Aug. 16, 2016, 8:01 AM), http://www.wired.com/2016/08/baltimore-pds-race-bias-extends-high-tech-spying; Colin Daileda, *The Police Surveillance Technology Intensifying Racial Discrimination*, MASHABLE (Oct. 3, 2016), http://mashable-com-cdn.ampproject.org/v/s/mashable.com/2016/10/03/police-technology-surveillance-racial-bias.amp.

[113] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); BATES, *supra* note 107, at 5.

[114] *See* Pell & Soghoian, *supra* note 4, at 147–48 (2013) ([T]he StingRay, masquerading as the cell site with the strongest signal, receives the information immediately and directly as it is communicated by the mobile phones, leaving no trace of the interception with the third party provider."); McCullough, *supra* note 111, at 42 (indicating that Stingrays do not involve third party service).

[115] Henry Bernstein, Comment, *The Need for Fourth Amendment Protection from Government Use of Cell Site Simulators*, 56 SANTA CLARA L. REV. 177, 204–205 (2016); Tom Winter et al., *Trail to Austin Bombing Suspect Combined High-Tech and Old-Fashioned Techniques*, NBC News (Mar. 21, 2018, 1:22 PM), https://www.nbcnews.com/news/us-news/trail-austin-bombing-suspect-combined-high-tech-old-fashioned-techniques-n858791 (last updated Mar. 21, 2018, 2:39 PM). *See also* Bates, *supra* note 107, at 8 (describing the Stingray's effective use in drug crime and terrorism investigations); Cox, *supra* note 4, at 30 (describing how numerous federal law enforcement agents in the Department of Justice, Department of Homeland Security, and Department of Treasury use Stingray technology).

[116] Robert Snell, *Feds Use Anti-Terror Tool to Hunt the Undocumented*, DETROIT NEWS (May 18, 2017, 10:49 PM), https://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/ (last updated May 19, 2017, 6:18 PM).

and $125,000.[117] The DOJ and DHS spent $95 million on more than 430 cell-site simulators from 2010–2014.[118] Homeland Security also earmarked $1.8 million to state local law enforcement agencies to buy them.[119]

Here lies the problem with Stingray use: often, Stingrays are not being used for investigations of serious crimes like murders, kidnappings, rapes, shootings, aggravated assaults with serious injuries, capturing fugitives, and robberies. To the contrary, Stingrays are used in run-of-the-mill matters such as locating stolen cell phones, or scanning from the skies over amusement parks and along the border.[120]

Absent any specified protocol about their Stingray use or judicial oversight, law enforcement freely relies on Stingrays to either target and track individual protests or to mass-collect phone numbers in high crime areas.[121] Such threats to individual privacy are arguably the equivalent of the broad and indiscriminate searches that the Fourth Amendment was intended to prevent. Yet these options were used by the Baltimore Police Department ("BPD") during the riots following the death of Freddie Gray at the hands of the Baltimore police, and during peaceful Black Lives Matter

---

[117] *See* Kate Klonick, *Stingrays: Not Just for Feds! How Local Law Enforcement Uses An Invasive, Unreliable Surveillance Tool*, SLATE (Nov. 10, 2014, 9:52 AM), http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law-enforcement_uses_an_invasive_surveillance.html.

[118] Snell, *supra* note 116.

[119] *See* Mike Maharrey, *Federal Programs are Funding Local Stingray Spying*, TENTH AMEND. CT (Aug. 26, 2017) https://tenthamendmentcenter.com/2017/08/26/federal-programs-are-funding-local-stingray-spying/.

[120] *See* George Joseph, *Racial Disparities in Police "Stingray" Surveillance, Mapped*, CITYLAB (Oct. 18, 2016), https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-sureveillance-mapped/502715/. David Gray suggests that the use of cell-site simulators should be limited to exceptional circumstances, and its use in routine surveillance be avoided. GRAY, *supra* note 8, at 262. The Anaheim police department regulars flies over Disneyland with a Stingray. *See* Kate Knibbs, *Disneyland's Local Police Force Caught Secretly Using Powerful Phone Spying Tools*, GIZMODO (Jan. 28, 2016, 10:04 AM) https://gizmodo-com.cdn.ampproject.org/v/gizmodo.com/disneylands-local-police-force-caught-secretly-using-po-1755671568/amp. ICE uses Stingrays to track down undocumented immigrants, and these devices can be mounted on airplanes at the border to look for illegal immigrants. Snell, *supra* note 116; Nathan Freed Wessler, *ICE Using Powerful Stingray Surveillance Devices In Deportation Searches*, AM. C.L. UNION (May 23, 2017, 10:15 AM), https://www.aclu.org/blog /privacy-technology/surveillance-technologies-ice-using-powerful-stingray-sureveillance-devices.

[121] Klonick, *supra* note 117. *See also* Andrew Guthrie Ferguson, *Crime and the Fourth Amendment: Redrawing "High-Crime Areas"*, 63 HASTINGS L.J. 179, 190–196 (2011) (describing how crime-mapping technology is reshaping Fourth Amendment protections in high crime areas and "hot spots" of crime); Andrew Guthrie Ferguson & Damien Bernache, *The "High Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis*, 57 AM. U.L. REV. 1587, 1590–92 (2008) (analyzing and critiquing reviewing courts' consideration of whether an area is a "high crime area" as a factor supporting the reasonableness of Fourth Amendment stops).

demonstrations.[122] This questionable use of Stingrays has become routine. The BPD—the heaviest user of Stingrays in the country—deployed Stingray cell simulators thousands of times in low-income African American sections of the city in ninety percent of Stingray incidents mapped.[123] Known Stingray operations in Milwaukee and Tallahassee are also heavily concentrated in poor communities of color.[124]

More to the point, an accurate and complete evaluation of the efficacy of Stingray programs cannot be achieved due to the lack of transparency about their purchase and use.[125] In addition, mounting pushback comes from judges and elected officials against the Stingray's unfettered use and the often cloak and dagger shenanigans that accompany it. For instance, when law enforcement submits applications for search warrants, they often disingenuously leave out any references to the use of cell-site simulators. When questioned, agencies using Stingrays are quick to half-heartedly explain that public revelation of their technological capabilities threaten to compromise the efficacy of surveillance.[126]

A more candid answer would explain that agencies cannot reveal such information because of the non-disclosure agreement ("NDA") required by the Florida-based Harris Corporation, the biggest manufacturer of Stingrays. It requires police departments and government agencies to sign extensive NDAs to prevent them from disclosing any information to the

---

[122] Barrett, *supra* note 112; Daileda, *supra* note 112; Martino, *supra* note 4.

[123] Barrett, *supra* note 112; Daileda, *supra* note 112; Joseph, *supra* note 120. Given Carpenter's narrow ruling, the use of technology by the police in minority communities is still an issue of concern. *See* Barry Friedman, *The Worrisome Future of Policing Technology*, NY TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/opinion/the-worrisome-future-of-policing-technology.html (arguing that *Carpenter* fails to allay fears of the increased use of technology by the police to target communities of color and marginalized people).

[124] *See* Joseph, *supra* note 120.

[125] Tom Jackman, *DC Appeals Court Poised to Rule On Whether Police Need Warrants for Cellphone Tracking*, WASH. POST (Apr. 18, 2017), https://www.washingtonpost.com/news/true-crime/wp/2017/04/18/d-c-appeals-court-poised-to-rule-on-whether-police-need-warrants-for-cellphone-tracking/?noredirect=on&utm_term=.964884aa3029 (reporting the secret use of cell-site simulators by police and federal agents over the years). *See also* Hemmer, *supra* note 105, at 301 (calling for the heightened judicial review of Stingray searches which infringe upon civil liberties); Bruce Vielmetti, *7th Circuit Rejects Appeal in Stingray Cases*, MILWAUKEE J. SENTINEL (Dec. 23, 2016, 3:44 PM), http://www.jsonline.com/story/news/blogs/proof-and-hearsay/2016/12/23/7th-Circuit-Rejects-Stingray-Appeal (last updated Dec. 23, 2016, 10:02 PM). The New York Civil Liberties Union sued the New York Police Department in 2016 for specific information on its Stingray program after a records request under the state's Freedom of Information law, but a New York city judge denied the request and ruled that information collected by Stingrays may remain confidential. Hetherly, *supra* note 111.

[126] *E.g.*, Vielmetti, *supra* note 125 ("Originally developed for national security, Stingrays have become a powerful tool for local police who promise the FBI they won't acknowledge having Stingrays to anyone else, including judges who might ask what led to a defendant's arrest.").

public or courts about their use of cell-site simulators and about the devices themselves.[127]

The government's reluctance, and sometimes outright refusal, to provide information about the capabilities of Stingray technology to the courts evokes great skepticism. This outlook heightens even more whenever the FBI requires state prosecutors to dismiss charges in civil and criminal cases to avoid revealing information about the use and full capabilities of Stingray technology.[128]

Understandably, there has been mounting outcry at the grassroots level against Stingray surveillance by public defenders and privacy activists, who demand that police be more transparent about the surveillance and that the public be allowed to participate in the decision-making process over how Stingrays are used.[129] At the legislative level, senators have called for transparency of Stingray policies. Perhaps these kinds of activism directly or indirectly influenced the DOJ's 2015 decision requiring federal investigators to obtain a warrant to use Stingrays.[130]

Outside the beltway, about one third of states have passed laws that protect citizens' cell phone data and require police to get a warrant to use a

---

[127] BATES, *supra* note 107, at 3, 6. *See also* FRIEDMAN, *supra* note 16, at 7, 31–33 (2017) (describing how police nationwide engage in "massive conspiracy to cover up the use of Stingray cell phone tracking technology" and referring to the FBI's requirement that its employees sign nondisclosure agreements); Cox, *supra* note 4, at 31 ("The FBI has imposed unusual constraints on how StingRay technology can be described in application for court orders or warrant nondisclosure agreements are required"); Owsley, *supra* note 4, at 200 ("[V]arious government agencies, both federal and state alike, have taken measures to keep their use of cell site simulators secret.").

[128] *See* Cox, *supra* note 4, at 32 (reporting speculation by commentators that state and federal charges have been reduced or dismissed by federal prosecutors in lieu of revealing confidential information about Stingrays to the court); Maharrey, *supra* note 119.

[129] Joseph, *supra* note 120.

[130] *See* Snell, *supra* note 116. Congress must also update and create privacy laws to address law enforcement's use of these advanced surveillance techniques. *See* Cox, *supra* note 4, at 35 (calling for Congress to draft legislation creating a new statutory right in privacy and limiting government's access to this data); *Congress Must Reckon with the Fourth Amendment and new technology*, WASH. POST (June 23, 2018), https// www.washingtonpost.com/amphtml/opinions/congress-must-reckon-with-the-fourth-amemdment-and-new-technology/2018/06/23/195578cO-7653-11c8-9780-bldd6a09b549_story_html (opining that after *Carpenter* Congress should step in to craft rules that clarify standards to accommodate new technology).

Stingray.[131] New York and other states are developing similar legislation.[132] On the local level, several cities and counties, including Berkeley, Oakland, and Seattle, have already adopted strong laws governing the police acquisition and use of surveillance technologies.[133]

But legislation may not be enough as Stingrays continue to threaten the reasonable expectation of privacy held by Americans when they use their cell phones.[134] Though half of Americans are willing to endure surveillance in the name of national security and fighting terrorism, it is unlikely that Americans would approve of the use of Stingrays by the police to spy on them—if they were even aware of their use.[135] Informing this is an amicus brief filed in *Carpenter* by empirical Fourth Amendment scholars, citing numerous studies reporting that a majority of people do not knowingly convey their location information to cell phone providers and expect law enforcement to obtain a warrant before gathering information.[136] Taking this analysis a step further, if the outrage over the recent breach of Facebook data is any indication, it is doubtful that Americans want to allow the government to be able to obtain private information about them.[137]

B. CALLS FOR A WARRANT REQUIREMENT FOR THE USE OF STINGRAY CELL-SITE SIMULATORS FROM LEGAL SCHOLARS

Just as the government is required to get a warrant for CSLI information pursuant to *Carpenter*, a warrant should also be required for

---

[131] *See, e,g.*, FRIEDMAN, *supra* note 16, at 101; Cox, *supra* note 4, at 31 (discussing the reaction by various state legislatures to the use of Stingrays and remarking that "[t]welve states have passed laws mandating that law enforcement's use of a cell site simulator must be based upon a court issued search warrant based upon a finding of probable cause."); Klonick, *supra* note 117; Mike Maharrey, *Missouri Committee Passes Bill to Ban Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMEND. CTR. (Feb. 21, 2018), http://blog.tenthamendmentcenter.com/2018/02. *See also* Snell, *supra* note 116 (proposing that states adopt laws requiring judicial authorization before local law enforcement is allowed to use Stingrays, limiting how long they can retain the data, and reserving their use only in cases implicating violence or harm to human life).

[132] Martino, *supra* note 4.

[133] *See* DJ Pangburn, *Berkeley Mayor: We Passed the "Strongest" Police Surveillance Law*, FAST COMPANY (Apr. 24, 2018), https://www.fastcompany.com/40558647/berkeley-mayor-we-passed-the-strongest-police-surveillance-law; Robyn Greene, *How Cities Are Reining in Out-of-Control Policing Tech*, SLATE (May 14, 2018, 1:58 PM), https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html.

[134] *See* Jackman, *supra* note 125.

[135] Klonick, *supra* note 117.

[136] *See* Brief of *Amici Curiae* Empirical Fourth Amendment Scholars in Support of Petitioner at 3–10, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

[137] *See* Singer, *supra* note 50.

Stingrays. A warrant requirement will deter intrusive and overbroad surveillance—a view supported by emerging Fourth Amendment scholarship about Stingray surveillance that warns of its use in undermining life in a free society.[138] First, in *Unwarranted: Policing Without Permission*, Professor Barry Friedman argues for transparency over the use of Stingrays and that law enforcement should be required to obtain a warrant before they are used to collect evidence from third parties.[139] In cases where the government claims that it cannot secure a warrant, Friedman asserts that the burden should be placed on them to fully explain their reasons.[140]

Second, Professor David Gray, in *The Fourth Amendment in an Age of Surveillance*, argues for more Fourth Amendment protection in the wake of new surveillance technologies:

> In light of the surveillance capacities of cell site simulators, their widespread use, the paucity of statutory regulations, and the utter absence of constitutional limitations . . . [i]t is hard to imagine a better example of conditions characteristic of a surveillance state or a means and matter of government surveillance more in need of Fourth Amendment regulation."[141]

Professor Gray prefers regulation of cell-site simulators via regulation resembling the Wiretap Act and limiting the use of cell-site simulators to exceptional circumstances.[142] This is a reasonable proposal. At a minimum, the government should be required to satisfy the exacting procedural requirements of the Wiretap Act before any Stingray use is authorized. Pursuant to the Federal Wiretap Act, before a wiretap can be issued a judge must find that "there is probable cause for belief than an individual is committing, has committed, or is about to commit" a crime.[143] The government must also show that the wiretap is necessary and that the goal

---

[138] *See* Laperuque, *supra* note 63.

[139] *See* FRIEDMAN, *supra* note 16 at 49, 257–58. The Electronic Frontier Foundation also advocates for courts to require a warrant based on probable cause and insists that cell-site simulators be used only for identifying locations in cases involving serious and violent crimes, and opposes the police use of Stingrays. *See Cell-Site Simulators: IMSI Catchers*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers (last visited May 21, 2019).

[140] FRIEDMAN, *supra* note 16, at 257–58.

[141] GRAY, *supra* note 8, at 38.

[142] *Id.* at 255.

[143] 18 U.S.C. § 2518(3)(a) (2012).

of the investigation could not be achieved through normal investigative techniques.[144]

Third, with regard to emerging technologies generally used by law enforcement, Professor Ferguson in *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* proposes that controls be placed on the design, implementation, and accuracy of data, arguing that a focus on accountability and transparency is critical.[145] Based on the research and reasoning offered by Friedman, Gray, and Ferguson, establishing a warrant requirement for using a Stingray would allow the police to comport with the Fourth Amendment without unreasonably burdening their ability to gather information.[146]

C. LEGAL AUTHORITY FOR A WARRANT REQUIREMENT FOR STINGRAY CELL-SITE SIMULATORS

Until the Supreme Court addresses the issue of cell-site simulators by the police, state supreme courts and federal courts, in the interim, can adopt the reasoning of *Carpenter* and review four state court decisions which have ruled against the use of Stingrays without warrants for the necessary

---

[144] *Id.* § 2518(4)(e). Requisite necessity cannot be shown by "bare conclusory statements that normal techniques would be unproductive . . ." United States v. Ashley, 876 F.2d 1069, 1072 (1st Cir. 1989). The affiant cannot rely on mere "boilerplate recitations of the difficulties of gathering usable evidence" in place of specific factual allegations explaining why a normal investigation will not succeed. United States v. Kerrigan, 514 F.2d 35, 38 (9th Cir. 1975); United States v. Blackmon, 273 F.3d 1204, 1210–11 (9th Cir. 2001) (holding that wiretap application affidavit contained "boilerplate assertions" that were "unsupported by specific facts relevant to the particular circumstances of [the] case" that "would be true of most if not all narcotics investigations.").

[145] *See* FERGUSON, *supra* note 50, at 188.

[146] For additional support in the legal community of a warrant requirement for Stingray technology, *see* Owsley, *supra* note 4, at 187 (proposing that applicable standard for granting request for using cell-site simulators should be based on Fourth Amendment probable cause standard and advocating for a protocol to be established for dealing with third party information capture by application for cell-site simulators); Bernstein, *supra* note 115, at 204(suggesting that "[a] warrant requirement would mitigate the risks of Stingray abuse . . . [and provide] judicial oversight into the use of the Stingray."); Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 534 (2017) ("Court oversight also prevents police from having more power to track a suspect under an arrest warrant than under a search warrant.").

analytical framework.[147] First, in *State v. Andrews*,[148] the Maryland Court of Special Appeals ruled on the issue of whether a cell phone's use as a real-time tracking device by the government without a warrant violated the Fourth Amendment.[149] It held that the Baltimore Police Department's use of Hailstorm, an upgraded version of the Stingray, required a valid search warrant based on probable cause.[150] The appellate court was the first state appellate court to order the suppression of evidence obtained by use of a Stingray.[151]

The Maryland Court of Special Appeals determined that the government violated the defendant's Fourth Amendment rights by using the Hailstorm to locate him, and that the State's actions in protecting the Hailstorm technology—driven by an NDA—was anathema to constitutional principles.[152] Of particular concern to the court was the potential for unchecked use of the Hailstorm to track a cell phone's movement across both public and private spaces to learn about the private and personal habits of any user.[153] The court determined that the defendant did not "assume the risk" that the information obtained through the use of the Hailstorm device would be shared by the service provider as in *Smith*.[154] It further concluded that the third-party doctrine did not apply since the defendant never voluntarily transmitted his location data to a third party.[155]

---

[147] *See generally* U.S. v. Ellis, 270 F. Supp. 3d 1134 (N.D. Cal. 2017) (stating that the Ninth Circuit has not decided the question whether the use of cell-site simulators to locate cell phones in real time amount to a search nor the issue whether there is a reasonable expectation of privacy in one's cell phone location). In a recent ruling, the federal district court in San Francisco held a defendant had a reasonable expectation of privacy in his real-time cell phone location, and the use of the Stingray devices to locate his phone amounted to a search, but denied the defendant's motion to suppress because the defendant failed to show a reasonable expectation or privacy in his public movement, and the movement was able to show that the exigent circumstances exception to the warrant requirement applied. *See* Tara Siler, *Bay Area Police Departments Using "StingRay" Surveillance Technology*, KQED NEWS (Mar. 14, 2014), https://www.kqed.org/news/129328/bay-area-police-departments-using-stingray-surveillance-technology (In the west, the Alameda County District Attorney's Office, and the police departments in Fremont, San Diego, San Francisco, San Jose, Oakland, Los Angeles, and Fremont use Stingrays.).

[148] State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

[149] *Id.* at 350.

[150] *Id.* Additionally, Barry Friedman explains that Stingrays have been used in Baltimore more than four thousand time from 2007 through 2015. FRIEDMAN, *supra* note 16, at 34.

[151] FRIEDMAN, *supra* note 16, at 34.

[152] *Andrews*, 134 A.3d at 338–39.

[153] *Id.* at 348.

[154] *Id.* at 352.

[155] *Id.*

Second, in a case of first impression, the District of Columbia Court of Appeals in *Jones v. United States*[156] ruled that the D.C. Metropolitan Police Department's warrantless use of Stingray technology in an investigation violated the Fourth Amendment.[157] The defendant was convicted of robbing three women and raping two of them.[158] During two of the attacks, he stole the cell phone of the victims.[159] Believing that the defendant would use the stolen phones, the police used a Stingray to track down the defendant and the second phone he stole.[160] The police argued that exigent circumstances permitted their warrantless use of the Stingray, and thus that a good-faith exception to the exclusionary rule should apply to its use.[161] However, the court rejected this argument, concluding that exceptions to the warrant requirement did not arise from cases "remotely like the present one—where the police, not acting pursuant to a seemingly valid warrant, statute, or court opinion, conducted an unlawful search using a secret technology that they had shielded from judicial oversight and public scrutiny."[162] It ultimately concluded that the use of a cell-site simulator to locate the defendant through his cell phone invaded his actual legitimate and reasonable expectation of privacy in his location information, thus constituting a search that generally requires a warrant.[163]

Third, *People v. Gordon*[164] was the first case to limit the use of Stingrays by the New York City Police Department ("NYPD"). There, the police secured a pen register/trap and trace order authorizing the use of a Stingray in a criminal investigation.[165] Subsequently, the defendant was located and arrested at an address gleaned from the Stingray.[166] The court determined that the government had improperly permitted the NYPD to intercept the suspect's cell phone signals via the Stingray, and that the police needed a warrant, based on probable cause, to use such "eavesdropping"

---

[156] Jones v. United States, 168 A.3d 703 (D.C. 2017).
[157] *Id.* at 707.
[158] *Id.* at 707–708.
[159] *Id.*
[160] *Id.* at 708.
[161] *Id.* at 719.
[162] *Id.* at 720.
[163] *Id.* at 714–15. In dissent, Judge Thompson opined that society is not prepared to recognize an expectation of privacy in a phone's location outside of the home, and accordingly, the defendant could not have held a reasonable expectation that the location of the cell phone would be private, given that he was "traveling on the public roads with a powered-on, stolen cell phone." *Id.* at 735, 738.
[164] People v. Gordon, 68 N.Y.S.3d 306, (N.Y. Sup. Ct. 2017).
[165] *Id.* at 309.
[166] *Id.* at 308.

technology.[167] It further reasoned that "[t]he failure to obtain a proper eavesdropping warrant here prejudiced the defendant since the most useful and needed information about his location was procured from the unlimited use of the cell site simulator."[168] This ultimately raised the bar in New York for the use of a surveillance device.[169]

Fourth, in *State v. Sylvestre*,[170] one of the first post-*Carpenter* cell-site simulator decisions, the Florida District Court of Appeal distinguished between law enforcement's indirect surveillance derived from collecting historical CSLI and its direct surveillance derived from the use of a Stingray. The court rejected the government's argument that a CSLI order permitted the use of a cell-site simulator in tracking down a robbery suspect's cell-phone location, and concluded that a warrant was necessary under *Carpenter*.[171] In ordering the suppression of all evidence gathered by the cell-site simulator, while allowing CLSI evidence, the court professed the true nature of cell-site simulators:

> With a cell-site simulator, the government does more than obtain data held by a third-party. The government surreptitiously intercepts a signal that the user intended to send to a carrier's cell-site tower or independently pings a cell phone to determine its location. Not only that, a cell-site simulator also intercepts the data of other cell phones in the area, including the phones of people not being investigated. If a warrant is required for the government to obtain historical cell-site information voluntarily maintained and in possession of a third-party, we can discern no reason why a warrant would not be required for the *more invasive* use of a cell-site simulator. [172]

In sum, when considered as a group *Andrews*, *Jones*, *Gordon*, and *Sylvestre* stand for the proposition that the warrantless use of Stingray technology by the government violates the Fourth Amendment.

V. CONCLUSION

As this article has hopefully shown, the Fourth Amendment continues to erode at the hands of law enforcement's continual exercise of unfettered

---

[167] *Id.* at 311.
[168] *Id.*
[169] *See id.*
[170] State v. Sylvestre, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018).
[171] *Id.* at 989–92.
[172] *Id.* at 991 (emphasis added) (citing Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018)).

discretion to stop drivers, search and detain people on the streets, and secretly track people through their phone use and data information. This has been exacerbated by new surveillance technologies, particularly cell-site simulators known as Stingrays. While *Carpenter* has shown promise that the Court will reconsider its Fourth Amendment jurisprudence in light of new surveillance technology, more needs to be done to truly protect the privacy rights of ordinary Americans. A good place to start is to require that the government obtain a search warrant, supported by probable cause, before it may use cell-site simulators. But ultimately, more accountability and transparency on the part of the police, along with concrete action by the people, the courts, and legislators, is necessary if we sincerely want to preserve what little is left of the Fourth Amendment in the wake of covert surveillance technology.