St. John's Law Review

Volume 93
Number 2 *Volume 93, 2019, Number 2*

Article 3

January 2020

Stingray Cell-Site Simulator Surveillance and the Fourth Amendment in the Twenty-First Century: A Review of The Fourth Amendment in an Age of Surveillance, and Unwarranted

Harvey Gee

BOOK REVIEW

STINGRAY CELL-SITE SIMULATOR SURVEILLANCE AND THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY: A REVIEW OF *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE,* AND *UNWARRANTED*

BARRY FRIEDMAN, *UNWARRANTED: POLICING WITHOUT PERMISSION*, NEW YORK: FARRAR, STRAUSS AND GIROUX, 2017. PP. 434.

DAVID GRAY, *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE*, NEW YORK: CAMBRIDGE UNIVERSITY PRESS, 2017. PP. 305.

HARVEY GEE[†]

INTRODUCTION

The police can secretly track your every physical movement, listen to your private conversations, and collect data from your cell phone—all without first getting a warrant based on probable cause, signed off by a judge. "WTF?!" you text. Indeed, this practice by law enforcement using portable Stingray cell-site simulators as digital surveillance tools has also raised the eyebrows of privacy advocates and state and federal courts across the country in the past few years.

[†] 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 Jacqueline Mancini, Anthony Nania, David Saldamando, Olivia Walseth, Jamie Zeevi, and the *St. John's Law Review* for invaluable feedback and assistance in the preparation of this Review.

Stingrays, sometimes also referred to as Triggerfish, IMSI Catchers, and Digital Analyzers, are the military grade cell-site simulators used by federal and local law enforcement to electronically track individuals suspected of criminal activity or to conduct mass surveillance on groups of unsuspecting people or particular areas.[1] Stingrays, which were originally developed for military and intelligence agencies for use overseas, act as phony cell phone towers by sending powerful electronic signals to all cell phones within their range to trigger an automatic response from nearby phones.[2] Truly, Stingrays epitomize how new technologies are transforming the experience, regulation, and definition of personal privacy today. Lacking guidance on this issue, courts must choose to apply, adapt, or reject settled doctrinal rules, and interpret recent United States Supreme Court decisions, in deciding whether the use of Stingrays violates the Fourth Amendment. Because Fourth Amendment surveillance cases tend to crawl along the appellate process at a snail's pace, it will likely take years for this issue to reach the Supreme Court. In the meantime, lower courts are left wrestling with the constitutionality of cell-simulator use, and legislatures continue to debate about their efficacy.

This Review discusses two timely and insightful books examining the changing relationship between privacy and the Fourth Amendment in the digital era. Part I discusses the tensions between the need to protect privacy rights and the slowly evolving legal landscape during a time of rapidly changing technology, to introduce David Gray's *The Fourth Amendment in an Age of Surveillance*.[3] His book explains how the Fourth Amendment, though embattled, can have a prominent role in

---

[1] *See* 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.

[2] *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register and Less Than a Wire Tap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 147–48 (2013) (claiming "the unmediated nature of StingRay technology makes it essentially 'invisible' in operation and leaves behind no retrievable trace that is subject to future detection" and that "the 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 interception with the third party provider").

[3] DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017). Gray is a Professor of Law at the University of Maryland, Francis King Carey School of Law.

twenty-first century discussions of privacy, technology, and surveillance.[4] Gray's analysis is engaged to broaden the conversation about Stingray technology. This section analyzes a sampling of the litigation over Stingrays and highlights the divergent, sometimes vibrant, opinions held by courts about the viability of *Katz v. United States*[5] in current Fourth Amendment jurisprudence.

Part II analyzes two important Stingray surveillance cases, *State v. Andrews*[6] and *United States v. Patrick,*[7] speculating further about a future Supreme Court case where a majority looks disfavorably upon law enforcement's use of Stingray surveillance technology. Part III shifts to discuss Barry Friedman's book, *Unwarranted: Policing Without Permission,*[8] to explore why better police accountability is needed in a modern world. Citizens want both safe neighborhoods and less police misconduct at a time when the police are conducting searches with neither warrants nor probable cause.[9] *Unwarranted* is a critical dissection of the debates about policing, and a clarion call to take responsibility. At the core, Friedman argues that limitations must be placed on the unfettered discretion afforded to the police when they conduct traffic stops and stop and frisks as well as when they use surveillance technology.

Part IV builds upon the background established by the *Age of Surveillance* and *Unwarranted* to present an argument that curbing police authority to arbitrarily stop individuals is now more difficult in light of *Utah v. Strieff*,[10] a wrongly decided decision dealing a serious blow to the exclusionary rule.

Part V discusses the unfettered discretion exercised by the Metropolitan Police Department of the District of Columbia ("MPD") when embarking on indiscriminate searches using

---

[4] Gray's book is divided into six sections, touching on the age of surveillance, the Fourth Amendment, and competing proposals and Fourth Amendment remedies.

[5] 389 U.S. 347 (1967).

[6] 134 A.3d 324 (Md. Ct. Spec. App. 2016).

[7] 842 F.3d 540 (7th Cir. 2016).

[8] BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION (2017). Friedman is a Professor of Law at New York University School of Law.

[9] Friedman's book is divided into three parts covering democratic policing, constitutional policing, and twenty-first century policing. Democratic policing addresses the police working in secret and an ineffective legislature and court. Constitutional policing analyzes the police conducting searches without warrants and probable cause, and discriminatory searches. Twenty-first century policing explores surveillance technology, counterterrorism, and national security.

[10] 136 S. Ct. 2056 (2016).

Veritrax GPS records to look for potential suspects who may be on supervised probation. This issue has received scant attention because the increase in the number of people on community supervision, or "mass supervision," through probation and parole is largely an afterthought.

I. THE *JONES* CASE AND THE STINGRAY SURVEILLANCE DEBATE

> "[Stingrays] haven't contributed anything meaningful to counterterrorism efforts. Instead, they have largely served as police surveillance and information sharing nodes for law enforcement efforts targeting the frequent subjects of police attention: Black and brown people, immigrants, dissidents, and the poor."[11]

Jones v. United States illustrates the delicate balancing of privacy rights with the need for police to investigate a crime.[12] In a 2017 case of first impression in Washington, D.C. challenging the warrantless use of cell-site simulator technology, Jones was convicted of robbing and raping two women.[13] Jones stole a cell phone from one of the women.[14] The MPD, without first getting a warrant, relied on a Stingray to track down the phone's location.[15] The cell-site simulator led the police to a row of cars parked near the Minnesota Avenue Metro Station where they found and arrested Jones.[16] Jones was convicted of various offenses "arising out of two alleged incidents of sexual assault and robbery at knifepoint."[17]

The MPD argued that a warrant was not necessary because there were exigent circumstances present.[18] The District of Columbia Court of Appeals ruled that the MPD's use of Stingray

---

[11] Mike Maharrey, *Oregon Bill Would Ban Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMENDMENT CENTER (Jan. 17, 2019), https://blog.tenthamendmentcenter.com/2019/01/oregon-bill-would-ban-warrantless-stingray-spying-help-hinder-federal-surveillance/ (quoting Nasser Eledroos, *Oops–Did Police Accidentically Reveal Unconstitutional Surveillance When They Tweeted a Screenshot?* AMERICAN CIVIL LIBERTIES UNION (Oct. 11, 2018, 6:30 PM), https://www.aclu.org/blog/free-speech/rights-protesters/oops-did-police-accidentally-reveal-unconstitutional-surveillance).

[12] 168 A.3d 703 (D.C. 2017).

[13] *Id.* at 707–08.

[14] *Id.* at 708.

[15] *Id.* at 707–09.

[16] *Id.* at 708–09.

[17] *Id.* at 707.

[18] *Id.* at 710–11.

technology violated Jones's Fourth Amendment rights.[19] Judge Beckwith, writing for the panel majority, determined that it was unconstitutional for the government to use a Stingray to find Jones before first obtaining a warrant based on probable cause.[20] Beckwith was especially concerned with the actively deceptive nature of the Stingray and the lack of applicable law on these devices.[21]

Judge Thompson argued in his dissenting opinion that society is not prepared to recognize an expectation of privacy in a phone's location, and thus Jones, "traveling on the public roads with a powered-on, stolen cell phone," could not have held a reasonable expectation that the location of the cell phone would be private.[22] In an aside, Thompson drew a distinction between cell phone owners' two-fold privacy expectations: people expect privacy in the actual contents saved in their cell phones, yet victims of cell phone theft would be willing to give up their expectation of privacy if a Stingray is used to track down their stolen phone.[23]

These opposing opinions about the extent of Fourth Amendment protection between the two Washington, D.C. jurists sets the stage for Gray's commentary in *Age of Surveillance* about big data information gathering, including the prevalence of cell-site simulators and their surveillance of almost all cell phones. Gray's commentary uncovers the original meaning of the Fourth Amendment to reveal its historical guarantees of collective security against threats of "unreasonable searches and seizures," and it ends with concrete solutions to the current Fourth Amendment crisis.

At the outset, indiscriminate big data information gathering by the government is prevalent. By definition, big data are "technologies and programs that aggregate, store, and analyze" varied source material.[24] Big data programs have access to information sources including credit histories, criminal records, property ownership, consumer transactions, and other personal

---

[19] *Id.* at 707.

[20] *Id.* The court ruled on the issue of whether the use of a cell-site simulator constituted a search, even though the trial court declined to do so; the trial court focused instead on the issues of standing, exigent circumstances, and inevitable discovery. *Id.* at 710.

[21] *Id.* at 720.

[22] *Id.* at 735–36 (Thompson, J., dissenting).

[23] *Id.* at 730, 737–38.

[24] GRAY, *supra* note 3, at 38.

information.[25] Big data's collection methodology "leverages modern information gathering, aggregation, storage, and analysis technologies."[26] Big data affects the abilities of subjects to control access to often personal and sensitive information, impacts freedom of movement—no fly lists, global-positioning-system tracking of probationers—and affects the "ability of people to get jobs, secure housing, and access credit."[27]

While "these kinds of restraints on freedom fall short of traditional full custodial arrests," Gray says they still are "seizures" because "they place persons in the grasps of state power."[28] He further asserts that the government's "unfettered discretion to deploy and use big data programs threatens the Fourth Amendment rights of the people to be secure in their persons, houses, papers, or effects against unreasonable search or seizure."[29] Through this lens, Gray considers Stingrays as the most notorious of the broad tracking technologies exploiting personal electronic devices.[30] Cell-site simulators engage in invasive searches when they indiscriminately monitor communication devices.[31] The deployment of Stingrays has become commonplace, and they are most prevalent in urban areas and "high crime" neighborhoods.[32]

The benign appearance of Stingrays disguises their invidious nature. Stingrays resemble large metallic radio transmitters, are the size of suitcases, and can be carried by hand, placed in a car, or mounted on a drone or airplane.[33] Stingrays capture text, numbers of outgoing calls, emails, serial numbers, identification information, GPS locations, actual contents of conversations, and other raw and detailed information from unsuspecting phones and they can track the locations of targets and non-targets in

---

[25] *Id.* at 41.
[26] *Id.* at 263.
[27] *Id.* at 264.
[28] *Id.*
[29] *Id.* at 263–75.
[30] *Id.* at 4, 33–34, 261–63.
[31] *Id.* at 261–62.
[32] *Id.* at 4–5.
[33] *See id.* at 33–34; Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 14–15 (2014); Lisa Bartley, *Investigation: Law Enforcement Use Secret 'Stingray' Devices to Track Cell Phone Signals*, ABC7 EYEWITNESS NEWS (Dec. 3, 2014), https://abc7.com/news/investigation-law-enforcement-use-secret-devices-to-track-cell-phone-signals/421190/.

apartments, cars, buses, and on streets.[34] They can even make the tracked device send text messages and make calls.[35] The collateral consequences resulting from their use includes the disruption of cell service to phones in the form of service outages, blocked and dropped calls, and the complete draining of a cell phone's battery.[36]

To be fair, there are legitimate uses of Stingrays. Stingrays have proven to be useful in tracking down dangerous fugitives on crime sprees, including the suspect responsible for four Texas bombings last year.[37] They are invaluable tools for intelligence gathering in terrorism cases when there is an immediate threat to human life and for other emergency situations. More often than not though, Stingrays are not being used for investigations of serious crimes like murders, kidnappings, rapes, shootings, aggravated assaults with serious injuries, capturing fugitives, and robberies.[38] On 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.[39]

---

[34] GRAY, *supra* note 3, at 34–35, 38.

[35] *See, e.g.*, Jeremy H. D'Amico, *Cellphones, Stingrays, and Searches! An Inquiry into the Legality of Cellular Location Information*, 70 U. MIAMI L. REV. 1252, 1296 (2016) (noting that these devices can "intercept" calls and text messages); Andrew Hemmer, *Duty of Candor in the Digital Age: The Need For Heightened Judicial Supervision of Stingray Searches*, 91 CHI.-KENT L. REV. 295, 296 (2016) (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, 41–42 (2016) (same); Pell & Soghoian, *supra* note 33, at 14.

[36] *See* 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 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.

[37] *See Inside The "Fatal Mistake" That Led Police to the Austin Parcel Bombing Suspect*, ABC NEWS (last updated Mar. 21, 2018, 10:38 PM), https://www.abc.net.au/news/2018-03-22/how-a-phone-steered-the-hunt-for-texas-parcel-bomber/9576040.

[38] *See* Marlan 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.

[39] *See* Ashley Carman, *Cops in Disneyland's Homeland Used Stingray Surveillance Devices*, VERGE (Jan. 28, 2016), https://www.theverge.com/2016/1/28/10859596/california-anaheim-disneyland-police-stingray-spy (describing Anaheim Police Department's use of Stingrays and "dirtbox" surveillance devices within range of sixteen million Disneyland visitors); George Joseph, *Racial Disparities in Police "Stingray" Surveillance, Mapped*, CITYLAB (Oct. 18, 2016),

Absent any specified protocol about their Stingray use or judicial oversight, law enforcement freely relies on Stingrays to either target and track particular individual protests or to mass collect phone numbers in high crime areas.[40] Such threats to individual privacy are arguably the equivalent of the intrusive and indiscriminate searches that the Fourth Amendment was intended to prevent. In spite of these concerns, the questionable use of Stingrays has become routine. The Baltimore Police Department, the heaviest user of Stingrays in the country, deployed Stingrays thousands of times in low-income African American sections of the city in ninety percent of Stingray incidents mapped during the riots following the death of Freddie Gray at the hands of the Baltimore police, and during Black Lives Matter demonstrations.[41] Known Stingray operations in Milwaukee and Tallahassee are also heavily concentrated in non-white, poor communities.[42]

Unfortunately, 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. Aware of this, judges and elected officials are pushing back more and more against their unfettered use and the often cloak-and-dagger shenanigans that come along with that.[43] For instance, when law

---

https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-sureveillance-mapped/502715/; *Stingray Tracking Devices: Who's Got Them?*, ACLU (Nov. 18, 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them (identifying Customs and Border Protection and Immigration and Customs Enforcement as known federal agencies using Stingrays).

[40] *See* 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 an area as a "high crime area" as an evaluation factor determining reasonableness of Fourth Amendment stops); 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.

[41] *See* Barrett, *supra* note 36; Daileda, *supra* note 36; Joseph, *supra* note 39; Andy Martino, *Black Lives Matter Activists are Convinced the NYPD Hacked Their Phones*, THE OUTLINE (Apr. 7, 2017, 1:30 PM), https://theoutline.com/post/1360/black-lives-matter-police-surveillance-the-cops-hacked-their-phones?.

[42] *See* Joseph, *supra* note 39.

[43] *See* Hemmer, *supra* note 35, at 300–01 (calling for heightened judicial review of Stingray searches which infringe upon civil liberties); Tom Jackman, *D.C. 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-

enforcement officers submit applications for search warrants, they often disingenuously leave out any references to the use of cell-site simulators.[44] When questioned, agencies using Stingrays are quick to halfheartedly explain that "public revelation of their technological capabilities threaten to compromise the efficacy of surveillance."[45] Sometimes when backed into a corner, agencies will just drop their prosecution rather than spill the beans about the Stingray and risk a breach of the manufacturer's mandatory non-disclosure agreement.[46] Gray responds by advocating for statutory regulations for cell-site simulators, along with a warrant requirement as a counterbalance to the unfettered discretion of law enforcement:

> 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 method of government surveillance more in need of Fourth Amendment regulation.[47]

Essentially, Gray wants cell-site simulator regulations that are akin to the Wiretap Act.[48] Friedman similarly argues for transparency over the use of Stingrays because they act as wiretaps.[49] Both are correct. At a minimum, the government should be required to satisfy the exacting procedural

---

cellphone-tracking (reporting the secret use of cell-site simulators by police and federal agents over the years); Spencer S. Hsu, *In District, Warrantless Tracking Requests Surge in Past 3 Years*, WASH. POST, (July 19, 2017), https://www.washingtonpost.com/local/public-safety/court-warrantless-requests-to-track-cellphones-internet-use-grew-sevenfold-in-dc-in-three-years/2017/07/18/b284ac32-6b36-11e7-9c15-177740635e83_story.html.

[44] *See* GRAY, *supra* note 3, at 36; *see, e.g.*, Hemmer, *supra* note 35, at 297 (noting that in one case, "the government failed to specify the technology that it intended to use in executing the search warrant, leaving out crucial details related to the device's invasiveness and likely impact on third parties").

[45] THE CATO INSTITUTE, STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE (Jan. 25, 2017), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa-809-revised.pdf.

[46] *See* GRAY, *supra* note 3, at 36 (2017) ("In cases where defendants have nevertheless discovered what is afoot, local prosecutors have gone so far as to drop criminal charges in order to avoid exposing the use of cell site simulators to judicial review."); Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FEDERALIST SOC'Y REV. 29, 31–32 (2016) (reporting that "Baltimore officials agreed to seek dismissal of . . . charges" rather than "compromis[ing] the technology" by allowing its use to be revealed in court); Joseph, *supra* note 39.

[47] GRAY, *supra* note 3, at 38.

[48] *See id.* at 262–63.

[49] FRIEDMAN, *supra* note 8, at 32.

requirements of the Wiretap Act before any Stingray use is authorized. Pursuant to the Federal Wire Tap Act, before a wiretap can be issued, a judge must find that "there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter."[50] The government must also show that the wiretap is necessary and that the goal of the investigation could not be achieved through normal investigative techniques.[51]

Here, Friedman is most persuasive in insisting that warrants based on probable cause be required of the government when applying for court orders.[52] The focus of Fourth Amendment analysis, Friedman says, should be shifted from the perspective of whether surveillance technologies threaten a reasonable expectation of privacy to law enforcements' unfettered use of Stingrays, which threatens the right of the people to be secure against unreasonable searches and seizures.[53] Gray is in agreement, and insists that "[g]ranting this kind of unfettered discretion would pose the same kinds of general threats to the security of the people against unreasonable searches posed by general warrants and writs of assistance."[54]

Gray and Friedman are not outliers on this issue. There is growing, vocal, grass-roots opposition against Stingray surveillance by public defenders and privacy activists demanding more transparency of police surveillance, and that the public be allowed to participate in the decisionmaking process regarding how Stingrays are used.[55] Many observers have called for

---

[50] 18 U.S.C. § 2518(3)(a) (U.S.C. 2012).

[51] *See id.* at § 2518(3)(c).

[52] FRIEDMAN, *supra* note 8, at 137.

[53] *See id.* at 258; *see also* Amir Nasr, *Poll: Little Trust That Tech Giants Will Keep Personal Data Private*, MORNINGCONSULT (Apr. 10, 2017), https://morningconsult.com/2017/04/10/poll-little-trust-tech-giants-will-keep-personal-data-private (discussing polls reflecting the skepticism held by Americans about the ability of internet service providers to keep their personal data private); Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CENTER (Mar. 28, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ (same with regards to social media providers).

[54] GRAY, *supra* note 3, at 262.

[55] *See* Joseph, *supra* note 39.

transparency of Stingray policies after the Justice Department's 2015 decision requiring federal investigators to obtain a search warrant from a judge to use the device.[56]

Outside the beltway, Arizona, California, Colorado, Florida, Illinois, Indiana, Maine, Maryland, Minnesota, Missouri, Montana, Tennessee, Utah, Virginia, Washington, and Wisconsin have passed laws that protect citizens' cell phone data, requiring police to get a warrant to use a Stingray.[57] The Oregon Senate is considering a proposed law that blocks the warrantless use of Stingrays to protect privacy rights.[58] Likewise, the Texas legislature is considering a warrant requirement for Stingrays, except in emergency situations.[59] New York and other states are

---

[56] *See* Cox, *supra* note 46, at 35 (calling for Congress to draft legislation creating a new statutory right in privacy and limiting government's access to this data); Robert Snell, *Feds Use Anti-Terror Tool to Hunt the Undocumented*, DETROIT NEWS (May 18, 2018), https://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/. Indeed, Congress should update and create privacy laws to address law enforcement's use of these advanced surveillance techniques. *See* Editorial Board, *Congress Must Reckon with the Fourth Amendment and New Technology*, WASH. POST (June 23, 2018), https://www.washingtonpost.com/opinions/congress-must-reckon-with-the-fourth-amendment-and-new-technology/2018/06/23/f95578c0-7653-11e8-9780-b1dd6a09b549_story.html (opining that after *Carpenter*, Congress should step in to craft rules that clarify standards to accommodate new technology).

[57] *See, e.g.*, Cox, *supra* note 46, at 31 (discussing the reaction by various state legislatures to the use of Stingrays and remarking, "[T]welve states have passed laws requiring law enforcement's use of a cell-site simulator must be based upon a court issued search warrant based upon probable cause"); Katherine M. Sullivan, *Is Your Smartphone Conversation Private? The Stingray Device's Impact on Privacy in Statutes,* CATH. U. L. REV. 388, 400 (2018) (arguing for more state legislation to protect privacy of citizens); Klonick, *supra* note 40; Mike Maharrey, *Arizona Committee Passes Bill to Prohibit Warrantless Stingray Spying,* TENTH AMENDMENT CENTER (Feb. 7, 2017), https://fromthetrenchesworldreport.com/arizona-committee-passes-bill-prohibit-warrantless-stingray-spying/182520; Mike Maharrey, *Missouri Committee Passes Bill to Ban Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMENDMENT CENTER (Feb. 21, 2018), https://blog.tenthamendmentcenter.com/2018/02/missouri-committee-passes-bill-to-ban-warrantless-stingray-spying-hinder-federal-surveillance/; Mike Maharrey, *Florida Committee Passes Bill to Ban Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMENDMENT CENTER (Feb. 7, 2018), https://blog.tenthamendmentcenter.com/2019/02/florida-committee-passes-bill-to-ban-warrantless-stingray-spying-help-hinder-federal-surveillance-2/; Snell, *supra* note 56 (offering that states can adopt laws requiring judicial authorization before local law enforcement is allowed to use Stingrays, adopt laws limiting how long they can retain the data, and reserving the use of Stingrays only for cases implicating violence or harm to human life).

[58] Maharrey, *supra* note 11.

[59] *See* Anna M. Tinsley, *Texas Lawmakers' Bills Would Limit Cellphone Trackers*, FORT WORTH STAR-TELEGRAM (Apr. 18, 2015), https://www.star-telegram.com/news/politics-government/article18868620.html.

developing similar legislation.[60] On the local level, Berkeley, Oakland, Santa Clara County, Nashville, Seattle, Somerville, and Davis have already adopted strong laws governing the police acquisition and use of surveillance technologies.[61] All told, these legislative measures are only the first steps in regulating Stingrays. As discussed below, legislation means nothing unless it has teeth and bite. Moreover, it must pass judicial muster and contain a warrant requirement.

II. ARGUING ABOUT STINGRAYS: MORE JUDGES DISAGREE ABOUT THE LEGALITY OF CELL-SITE SIMULATORS

This section looks at two important stingray surveillance cases that were precursors to *Jones v. United States*. Some Maryland jurists are disdainful about the use of Stingrays, while some Chicago judges conclude that Stingrays are not invasive.

A. Lower Courts Wrestle Onward About the Constitutionality of Stingray Surveillance

In *State v. Andrews*, the Maryland Court of Special Appeals ruled in 2016 on whether the government may transform a cell phone into a real-time tracking device without a warrant, and the court 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.[62] The appellate court was the first state appellate court to order evidence obtained using a Stingray to be suppressed.[63] As with most cell-site location information ("CSLI") cases, the government relied on the third-party doctrine established by *United States v. Miller*, which concerned bank records,[64] and *Smith v. Maryland*,

---

[60] Martino, *supra* note 41.

[61] *See* Robyn Greene, *How Cities Are Reining in Out-of-Control Policing Tech*, SLATE (May 14, 2018), https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html; 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.

[62] State v. Andrews, 134 A.3d 324, 350 (Md. Ct. Spec. App. 2016).

[63] *See* Cyrus Farivar, *For the First Time, Federal Judge Tosses Evidence Obtained Via Stingray*, ARS TECHNICA (July 12, 2016, 9:07 PM), https://arstechnica.com/tech-policy/2016/07/for-the-first-time-federal-judge-tosses-evidence-obtained-via-stingray/.

[64] 425 U.S. 435, 438–40 (1976). In *Miller*, federal agents presented subpoenas to two banks to produce financial records of the defendant. *Id.* at 437. The Court held that the Fourth Amendment was not violated because there was no reasonable

which concerned pen registers.[65] Under the third-party doctrine, when information is "voluntarily" given to third parties, an individual has no reasonable expectation of privacy in that information, making the Fourth Amendment inapplicable.[66]

The Maryland Court of Special Appeals found that the government violated the defendant's Fourth Amendment rights by using the Hailstorm to locate him. The court viewed the State's actions in protecting the Hailstorm technology with the use of an non-disclosure agreement as contrary to constitutional principles.[67] 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.[68] The court concluded that (1) Andrews did not "assume the risk" that the information obtained through the use of the Hailstorm device would be shared by the service provider and that (2) the third-party doctrine did not apply since his location data was never transmitted to a third-party—such as a cell-service provider—voluntarily by Andrews.[69]

That same year, the the Seventh Circuit sided with the government's use of Stingrays in *United States v. Patrick*,[70] which was the first time that a federal court substantively discussed the warrantless use of a Stingray. Wisconsin police arrested Damian Patrick while he was in a car on a public street and in unlawful possession of a gun.[71] Patrick, a state prison parolee, had a warrant issued for his arrest for noncompliance with the conditions of his release.[72] Milwaukee police found Patrick with

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 442–43.

[65] 442 U.S. 735, 745–46 (1979). In *Smith*, police officers were attempting to track down a robber who had begun making obscene and harassing phone calls. *Id.* at 737. The Court concluded that there was no reasonable expectation of privacy in pen registers. *Id.* at 745–46.

[66] *See Andrews*, 134 A.3d 324, 350–51 (2016).

[67] *See id.* at 338.

[68] *Id.* at 348.

[69] *Id.* at 398–99.

[70] 842 F.3d 540 (2016).

[71] *Id.* at 541.

[72] *Id.* at 542.

the use of cell phone data that was authorized by a second warrant.[73] Patrick's location had been pinned down using data from a Stingray.[74]

After the state conceded that the use of a cell-site simulator was a search, Patrick argued that the location-tracking warrant was invalid because police were required to obtain a warrant, and that police should have revealed to the state judge who issued the location-tracking warrant about the Stingray.[75] In affirming Patrick's conviction, the panel majority punted on the substantive questions about whether a warrant is required to use the Stingray and whether a cell-site simulator is a reasonable means of executing a warrant.[76] The panel 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.[77] In making that determination, the panel majority paid deference to law enforcement's assurances that Stingrays are not invasive, merely relying on the Department of Justice Policy Guidance manual's boilerplate disclaimer that cell-site simulators do not function as a GPS locator, do not capture emails, texts, contact lists, images, or other phone data, and do not provide subscriber account information.[78] The panel mischaracterized the prowess of Stingrays when it suggested that Stingrays only provide the same kind of information that can be obtained from a phone company.[79]

The majority panel's glossing over the dangers of Stingray surveillance seemingly raised the ire of dissenting Chief Judge Dianne Wood, who argued that the panel underestimated the Stingray's capabilities.[80] She was especially critical of: (1) the government's unwillingness to be forthcoming with information about how the Stingray was used; (2) its concealing the use of the Stingray when seeking the warrant; and (3) the majority panel's "blind reliance" on the Department of Justice manual assumption that the Milwaukee police followed proper procedures.[81]

---

[73] *Id.*
[74] *Id.*
[75] *Id.* at 543–44.
[76] *Id.* at 545.
[77] *Id.*
[78] *Id.* at 543.
[79] *Id.* at 543–44.
[80] *See id.* at 545 (Wood, J., dissenting).
[81] *Id.* at 546–47.

In light of these serious concerns, Chief Judge Wood wanted to remand the case for further fact finding concerning the Wisconsin police's reliance on the Stingray and the authorization for searching Patrick's cell phone:

> It is time for the Stingray to come out of the shadows, so that its use can be subject to the same kind of scrutiny as other mechanisms, such as thermal imaging devices, GPS trackers, pen registers, beepers, and the like. Its capabilities go far beyond any of those, and cases such as *Riley* indicate that the Supreme Court might take a dim view of indiscriminate use of something that can read texts and emails, listen to conversations, and perhaps intercept other application data housed not just on the target's phone, but also those of countless innocent third parties.[82]

B. Reasons Why the Supreme Court Would Require a Warrant for the Use of Stingray Surveillance Technology

This subsection expands on Chief Judge Wood's advisement that a future Court case may look disfavorably upon law enforcement's use of Stingray surveillance technology. Relying on the pathways paved in prior key government surveillance rulings for direction—*Kyllo v. United States*,[83] *United States v. Jones*,[84] *Riley v. California*,[85] and *Carpenter v. United States*[86]—I predict that a majority will hold that law enforcement's use of cell-site simulators is subject to the Fourth Amendment, and a warrant is required for their use.

A brief survey of the Court's important surveillance cases of the past two decades supports this belief. In the 2001 decision *Kyllo v. United States*,[87] the Court held that the use of a thermal imaging device, aimed at a private home from a public street to detect relative amounts of heat and obtain information about the interior of a home, constitutes a "search" under the Fourth Amendment.[88] In 2012, in *United States v. Jones*,[89] a unanimous

---

[82] *Id.* at 552.

[83] 533 U.S. 27 (2001).

[84] 565 U.S. 400 (2012).

[85] 573 U.S. 373 (2014).

[86] 138 S. Ct. 2206 (2018).

[87] 533 U.S. 27 (2001).

[88] *See also* Andrew G. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions,* 65 LAW & CONTEMP. PROBS. 125, 133 (2002) ("The Supreme Court has generally failed to see any enhanced dangers to privacy caused by rapidly changing police surveillance technologies. . . . [T]he Court has addressed technology questions under the same

Court expressed discomfort with the government's attachment of a GPS tracker on a jeep for twenty-eight days, which was determined to be a "search."[90] In the 2014 consolidated case *Riley v. California*,[91] the Court addressed whether an officer's search of a defendant's "smart phone" incident to an arrest violated the Fourth Amendment, and the Court ruled unanimously that police generally must obtain a warrant to search the contents of cell phones.[92] While each case involved distinct technology and different facts, their collective rationale fit together.

Then, *Carpenter v. United States* brought *Katz v. United States*[93] into the digital era by holding for the first time that a person has an expectation of privacy in the whole of his or her physical movement, and that law enforcement agencies generally need a warrant to track suspects' locations using CSLI.[94] Chief Justice Roberts, joined by Justices Ginsburg, Breyer, Sotomayor, and Kagan, ruled that cell phone users possess a reasonable expectation of privacy in the CSLI history associated with their cell phones.[95] Accessing a person's historical cell-site records, or at least seven days or more of cell-site records, is a Fourth

---

analytical framework that it uses for resolving all Fourth Amendment search questions.").

[89] 565 U.S. 400 (2012).

[90] *Id.* at 406. Justice Scalia sidestepped the issue of applying *Katz* and instead used common law trespass theory to conclude that the Government "trespassorily" inserted the information gathering device when it encroached on Jones's jeep—a protected area. *Id.* at 409, 411–12.

[91] 573 U.S. 373 (2014).

[92] *Id.* at 403. The majority recognized the privacy interests in the kinds of vast data stored in modern cell phones that are so persuasive today. *Id.* Cell phones contain information about internet searches and browsing history and can reveal enough personal information and private interests, in the aggregate, to reconstruct a person's private life. *Id.* at 395–96. Cell phones are miniature computers that function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers" and possess great storage capacity, including the ability to record data even before their purchase date. *Id.* at 393–94. A cell phone's capacity also allows an individual's private life to be pieced together through dated and detailed photos, which can be reconstructed through a thousand photographs labeled with details. *Id.* at 394.

[93] Katz v. United States, 389 U.S. 347, 351–53 (1967). Fifty-year-old *Katz* superseded the prior Court rulings that defined "search" and "seizure" only in physical terms. Under the *Katz* two prong expectation of privacy test, a search within the meaning of the Fourth Amendment takes place when the defendant manifests an actual expectation of privacy that society is willing to recognize as legitimate, justifiable, or reasonable. *See id.* at 353.

[94] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[95] *Id.* at 2217–18.

Amendment search because it violates the person's "legitimate expectation of privacy in the records of his physical movements."[96] The *Carpenter* majority boldly rejected the government's arguments that people lose their privacy rights when using these technologies. In doing so, the majority reframed the third-party doctrine by limiting and departing from a tradition of deference paid to the doctrine and declined to extend it to cover CSLI.[97]

Importantly, Chief Justice Roberts raised concerns in dicta about the current and future potential for abuse if the government is able to collect a week or more of a person's data without having to show probable cause.[98] He pointed out that tracking historical cell-site records is much worse than GPS monitoring and more invasive.[99] Chief Justice Roberts's reasoning can be readily applied to Stingrays, which can identify a person's location *within six feet*, whereas CSLI location information only identifies a person's location within about a

---

[96] *Id.* at 2217.

[97] *Id.*; *see* Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAW FARE BLOG (June 22, 2018), http://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision. The Fourth Amendment safeguards should apply whenever citizens convey personal information to a third party under the promise of confidentiality; indeed the courts should "restore the Fourth Amendment to its intended position as a mechanism for preserving those spaces in the face of unprecedented technological, social, and political pressures." STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 143 (2012). The Government argues that the doctrine facilitates its ability to obtain information in criminal and terrorism investigations via subpoenas, which unlike warrants, do not require a showing of probable cause. FRIEDMAN, *supra* note 8, at 241. The government only needs to provide "specific and articulable facts" to a court, showing the information is potentially "relevant and material" to the criminal investigation. *Id.* at 245. Friedman suggests that law enforcement should be required to demonstrate how its investigation would be severely hampered before it is granted access to this private information held by third parties. *Id.* at 257. This can be facilitated by transparent rules governing the police's use of new technology, created after public discussion and debate. *Id.* at 326.

[98] *Carpenter*, 138 S. Ct. at 2221–22; *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), 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 Chief Justice Roberts's reliance in *Carpenter* on Justice Sotomayor's concurrence in *Jones* as reflected in his repeated citations to her concurrence).

[99] *Carpenter*, 138 S. Ct. at 2218.

half-mile.[100] As Professor Susan Freiwald and former federal magistrate judge Stephen W. 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, and so the third party doctrine of *Miller* and *Smith* is not even arguable here. 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. Perhaps for these reasons it has been DOJ policy since 2016 to seek a Rule 41 warrant to authorize use of these devices. Based on such legal and practical concerns, law enforcement use of cell site simulators will in all likelihood be subject to the Fourth Amendment.[101]

A similar outlook was embraced by one Florida appellate court that extended *Carpente*r's warrant requirement to a cell-site simulator to suppress evidence gathered by a cell-site simulator.[102] Unlike the *Patrick* panel majority, this court saw 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 or 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.[103]

Therefore, based on this analysis, one can reasonably anticipate that the Court would require the government to get a warrant before using a Stingray. Such a ruling would be a

---

[100] THE CATO INSTITUTE, STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE (Jan. 25, 2017), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa-809-revised.pdf.

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

[102] State v. Sylvestre, 254 So. 3d 986, 991–92 (Fla. Dist. Ct. App. 2018).

[103] *Id.* at 991 (citation omitted) (emphasis added).

natural extension of *Carpenter*. More importantly, the decision would be congruent with the original purpose of the Fourth Amendment.

C. Towards Mass Incarceration: Syncing Digital Surveillance Technology with the War on Drugs

For the most part, legal scholars have analyzed the Court's surveillance cases solely for their legal precedent and analytical framework about the government's use of high-tech tools. Few discuss them in a focused narrative about the use of unfettered discretion by law enforcement in the urban "War on Drugs." Upon a closer examination, the associated themes of narcotics, gangs, and race are at the forefront. First, *Kyllo* involved the police using an infrared thermal imaging device to scan a suspect's home from a city street.[104] The scanning revealed that the roof over Kyllo's garage was unusually hot—indicating to the government that the suspect was growing marijuana under heat lamps in the garage attic.[105] Second, the respondent in *Jones* was the owner and operator of a nightclub, who came under suspicion of trafficking drugs and became the target of a federal and local investigation.[106] Jones was convicted of conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and fifty grams or more of cocaine base.[107]

Third, in the consolidated cases of *Riley*, Riley was stopped by police officers for a routine traffic stop and subsequently arrested after his car was impounded and firearms found.[108] The officers accessed information from his smart phone showing that Riley was a member of a street gang.[109] In its companion case, Wurie was arrested for selling drugs after officers opened his phone and accessed its call log, tracing the number to his suspected apartment building.[110] Fourth, bands of robbers in *Carpenter* held up nine Radio Shack and T-Mobile cell phone

---

[104] Kyllo v. United States, 533 U.S. 27, 27 (2001).
[105] *Id.*
[106] United States v. Jones, 566 U.S. 400, 402 (2012).
[107] *Id.* at 403–04.
[108] Riley v. California, 573 U.S. 373, 378 (2014).
[109] *Id.* at 378–79.
[110] *Id.* at 373.

stores, and Carpenter was apprehended after one of the suspects gave police the names and cell phone numbers of his fifteen accomplices.[111]

The defendants in those cases were fortunate to be vindicated at the Supreme Court. But the vast majority of cases in the mass incarceration pipeline never get that far. Starkly, the war on drugs fueled the incarceration boom that has culminated in approximately 2.3 million people confined in federal and state prisons and local jails.[112] According to the *New York Times*, "[i]n 2010, more than 7 in 100 black men ages 30 to 34 years old were behind bars. The federal system alone holds 219,000 inmates, 40 percent above its capacity . . . ."[113] Crack cocaine violations are the most notorious enhanced penalty. Michelle Alexander characterizes mass incarceration as a new racial caste system and argues that addressing the disparity of racial bias in crack sentencing "is just the tip of the iceberg" because the caste system depends on the prison label affixed to felons, not the time they served in prison.[114] The felon label precludes a felon from employment and access to housing, as well as enjoying the privileges of citizens, such as voting and jury service.[115] "Those labeled felons will continue to cycle in and out of prison, subject to perpetual surveillance by the police, and unable to integrate into the mainstream society and economy."[116] Clearly these are the effects of mass incarceration.

III. RACE AND POLICE ACCOUNTABILITY IN A SURVEILLANCE STATE

This section explores why better police accountability is needed in a modern world that tries to balance the interests of citizens wanting safe neighborhoods with the interest of the police conducting investigations. It combines the analytical

---

[111] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[112] *See* KARA GOTSCH, BREAKTHROUGH IN U.S. DRUG SENTENCING REFORM: THE FAIR SENTENCING ACT AND THE UNFINISHED REFORM AGENDA 1 (2011), https://www.wola.org/sites/default/files/downloadable/Drug%20Policy/2011/FSA/WOLA_RPT_FSA-Eng_FNL-WEB.pdf.

[113] Editorial, *Smarter Sentencing*, N.Y. TIMES (Aug. 14, 2013), https://www.nytimes.com/2013/08/14/opinion/smarter-sentencing.html.

[114] *See* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS 139 (2010); *see also* Dorothy E. Roberts, *The Social and Moral Cost of Mass Incarceration in African American Communities*, 56 STAN. L. REV. 1271, 1304 (2004).

[115] ALEXANDER, *supra* note 114, at 191–94.

[116] *Id.* at 95–96.

framework offered by *Age of Surveillance* and *Unwarranted*: twenty-first century government surveillance involves technology and a dramatic increase in "stop and frisks" in urban areas, with aspects of critical race theory to better understand the gateway to mass incarceration.

A. Terry *and Racial Profiling on the Streets*

Every public defender grimaces at how, under *Terry v. Ohio*, police officers may stop and search and conduct routine searches and seizures under the guise of "reasonableness."[117] Officers need only point to some objective facts or observations that are sufficient to show reasonable suspicion under the circumstances; afterwards, courts then assess the reasonableness of searches and seizures from this objective point of view.[118] *Terry* was a landmark decision protecting defendants' rights, but, in the intervening fifty years, it has become increasingly unclear when stops are permissible.

Today, officers have broad and completely unfettered discretion to conduct searches and seizures, since the requirement to demonstrate reasonable suspicion of criminal wrongdoing has been diluted very much since *Terry*. The police can justify a decision to stop and frisk regardless of their true motivation, and courts tend to give them the benefit of the doubt.[119] In addition, the many Fourth Amendment exceptions the Court has carved out—such as those involving automobile stops, immigration laws, administrative searches, collecting and searching computer data, and DNA testing—have essentially neutralized the Fourth Amendment.[120]

At bottom, *Terry* has been frequently used to support the use of proactive stop and frisks by police with near impunity.[121] Friedman describes the dilemma: (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 the stopping

---

[117] Terry v. Ohio, 392 U.S. 1, 9 (1968).

[118] *See* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: CASES AND COMMENTARY 198 (8th ed. 2007) (explaining "[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").

[119] GRAY, *supra* note 3, at 279.

[120] *See* FRIEDMAN, *supra* note 8, at 167–68.

[121] *See id.*; GRAY, *supra* note 3, at 279.

and frisking, along with the officer's explanation for what constituted articulable suspicion for the stop.[122] As such, Gray cautions 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."[123] Indeed, "policing methods like stop and frisk have grown out of control, subjecting hundreds of thousands of innocent citizens to routine searches and seizures."[124]

Any meaningful discussion of *Terry* and modern search and seizure law must consider the intractability of race and the Fourth Amendment. The connection between the historical racial discrimination in American law enforcement and modern Fourth Amendment jurisprudence is strong. Carol Steiker asserts the Framers did not foresee how industrialization would spike racial animosity between black and white communities.[125] Nor did they predict the evolution of racially divisive modern law enforcement practices, and the Court's attendant shift to probable cause and the exclusionary rule.[126]

Surely police, emboldened by a lax Fourth Amendment jurisprudence favoring them, are disproportionately stopping persons of color more than white people.[127] This practice is the outgrowth from aggressive policing rooted in the forty-year war on drugs that began with Richard Nixon's 1971 professed offensive against hard drugs, which continued through the 1980s crack cocaine epidemic.[128] Alexander 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

---

[122] *See* FRIEDMAN, *supra* note 8, at 154–56.

[123] GRAY, *supra* note 3, at 279; *see* Paul Butler, *Stop and Frisk and Torture-Lite: Police Terror of Minority Communities*, 12 OHIO ST. J. OF CRIM. LAW 57, 57 (2014) ("Stop and frisk is, in the United States, a central site of inequality, discrimination, and abuse of power.").

[124] GRAY, *supra* note 3, at 279.

[125] Carol Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 839 (1994).

[126] *Id.* at 844–45.

[127] *See* FRIEDMAN, *supra* note 8, at 61–62.

[128] *See* JAMES FORMAN JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 20 (2017) (explaining that the drug war began with Richard Nixon's 1971 declaration of implementing "a new, all-out offensive" against hard drugs); Editors of Encyclopaedia Britannica, *War on Drugs*, ENCYCLOPAEDIA BRITANNICA (Dec. 5, 2018), https://www.britannica.com/topic/war-on-drugs (summarizing how the federal government escalated the war on drugs during the crack cocaine epidemic of the 1980s).

> Fourth Amendment protections against unreasonable searches and seizures have been eviscerated. Stop-and-frisk operations in poor communities of color are now routine; the arbitrary and discriminatory police practices the framers aimed to prevent are now commonplace.[129]

Set in this socio-historical-political context, Friedman's chapter "*Discriminatory Searches*" is especially engaging and covers the controversy over the racial profiling of racial minorities by law enforcement.[130] Dubiously, courts have allowed racial profiling as long as race is not the only factor for the profiling.[131] Consequently, the Fourteenth Amendment's Equal Protection Clause is effectively overridden in Fourth Amendment cases. Racial profiling is a byproduct of unconscious racial bias, which is to blame for the pervasiveness of racial profiling, more so than general intentional racism.[132] But racial profiling is ineffective as a policy because studies show that racial minorities do not use or possess drugs more than white people do.[133]

Gray also addresses racial profiling. The thrust is felt in Gray's argument that stop and frisk programs are ineffective and disproportionately target politically and economically vulnerable communities of color facing routine threats of being stopped and frisked. "This is a circumstance wholly contrary to the imperative command at the heart of the Fourth Amendment that the right of the people to be secure against unreasonable searches and seizures shall not be violated."[134] Even if aggressive stop and frisk programs were effective, they thwart the Fourth Amendment's goal of limiting government authority to conduct searches and seizures.[135] Aware of such concerns, Christopher Slobogin, in a complimentary analysis, proposes a return to *Terry*'s conceptual framework that is consistently and seriously

---

[129] Michelle Alexander, *The New Jim Crow*, AMERICAN PROSPECT (Dec. 6, 2010), https://prospect.org/article/new-jim-crow-0*; see also* Paul Butler, *The System is Working the Way it is Supposed to*: *The Limits of Criminal Justice Reform*, 104 GEO. L.J. 1419, 1428–36 (2016) (describing the racial injustices articulated by the Movement for Black Lives); Devon W. Carbado, *Blue-on-Black Violence: A Provisional Model of Some of the Causes,* 104 GEO. L.J. 1479, 1485–508 (2016) (listing factors which render African Americans vulnerable to repeated police interactions, including policing practices, mass criminalization, racial stereotyping, and racial segregation).

[130] FRIEDMAN, *supra* note 8, at 185.

[131] *Id.* at 198.

[132] *See id.* at 197.

[133] *Id.* at 197 (citing to different studies conducted).

[134] GRAY, *supra* note 3, at 276.

[135] *Id.* at 278.

enforced by courts with regards to all searches and seizures.[136] The Court could lead the way by developing a multitiered justification hierarchy with probable cause at the top, reasonable suspicion in the middle, and relevance resting at the bottom.[137]

To be sure, moving beyond the limiting totality-of-the-circumstances standard surrounding a police encounter will allow a deeper understanding of racial profiling. As a starting point, application of critical race theory to Fourth Amendment cases and issues brings race to the surface, offering insights about the power dynamics, attitudes, and behaviors between the officer and the person confronted. Devon Carbado and Daria Roithmayr heighten this analysis even further by suggesting critical race theory can be applied along with social science to show how African Americans are racialized as criminals through media representation and popular discourse.[138] Moreover, they question whether color-blind laws and social policy purporting to be race neutral actually undermine the interests of racial minorities.[139] Such an approach considers the realities of street policing.[140]

On this theme, critical race theorist Paul Butler describes how police actually patrol poor black neighborhoods with "violence" in the form of beating, killing, pepper spraying, stopping and frisking, and handcuffing African American men.[141]

---

[136] Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1054–55 (1998).

[137] *See id.* at 1053, 1081–85 (proposing a hierarchy of searches and seizures to be used based on the proportionality principle).

[138] *See* Devon W. Carbodo & Daria Roithmayr, *Critical Race Theory Meets Social Science*, 10 ANNU. REV. L. & SOC. SCI. 149, 151 (2014).

[139] *Id.* These theories can be grounded by practical applications. For example, in addressing systematic racial biases, the late San Francisco Public Defender Jeff Adachi 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, and community bridge building. *See generally* Jeff Adachi et al., *A Proposal to Achieve Racial Justice Through Enhancing the Work of Public Defense Organizations Throughout the Country*, BLUEPRINT FOR RACIAL JUSTICE, https://sflawlibrary.org/sites/default/files/Racial%20Justice%20Blueprint_1.pdf.
Such efforts would address the overrepresentation of racial minorities in San Francisco's criminal justice system by raising racial justice issues in jury selection and *voir dire*, bail charging, selective prosecution, racial profiling, and sentencing. *Id.*

[140] *See* Tracey Maclin, *"Black and Blue Encounter"—Some Preliminary Thoughts About Fourth Amendment Seizure: Should Race Matter?* 26 VALPARAISO U. L. REV. 243, 248, 250, 252, 253 (1991).

[141] *See generally* PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN 82–116 (2017).

These examples of police misconduct were neatly encapsulated for mainstream America through media accounts of the violent killings of young African American men following the 2012 shooting of African American seventeen-year-old Trayvon Martin in Miami Gardens, Florida and the 2014 shooting of eighteen-year-old Michael Brown in Ferguson, Missouri.[142] In the following years, there was a slew of tragic deaths of young black men and women at the hands of white police officers, accompanied by the Black Lives Matter demonstrations clamoring for police accountability.[143] Concerning this, Butler theorizes that police routinely harass and discriminate against African Americans so they can be placed under government surveillance.[144] He states, "[S]top-and-frisk does not make communities safer. Instead it causes many men of color to hate the police, and makes them less willing to engage with the government in any way . . . ."[145]

To supplement their academic discourse, Butler, Gray, and Friedman separately analyze the New York City Police Department's ("NYPD") use of stop and frisks, which was found to be unconstitutional by Judge Shira Scheindlin in 2013.[146] The NYPD made 4.4 million stops between January 2004 and June 2012.[147] As distilled from Judge Scheindlin's robust opinion, over eighty percent of those stopped were African American or Hispanic, and only ten percent of those stopped were white.[148] An equally damning statistic: fifty-two percent of the stops included a protective frisk for weapons, and only 1.5% of the frisks revealed a weapon.[149] African Americans and Hispanics were also more likely than whites to be subjected to the use of force.[150] Based on these findings, Judge Scheindlin concluded

---

[142] *See id.* at 61; ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 21–24 (2017); *see also* CNN, *Trayvon Martin Shooting Fast Facts*, CNN (last updated Feb. 28, 2019), https://www.cnn.com/2013/06/05/us/trayvon-martin-shooting-fast-facts/index.html.

[143] *See* BUTLER, *supra* note 141, at 61; FERGUSON, *supra* note 142. Those killed included Eric Garner, Tamir Rice, Freddie Gray, Laquan McDonald, Rekia Boyd, Remnisha McBride, and Walter Scott. *See* JEFF CHANG, WE GON' BE ALRIGHT: NOTES ON RACE AND RESEGREGATION 127 (2016).

[144] BUTLER, *supra* note 141, at 4, 8.

[145] *Id.* at 96.

[146] Floyd v. City of New York, 959 F. Supp. 2d 540, 667 (S.D.N.Y. 2013).

[147] *Id.* at 556.

[148] *Id.* at 556, 574.

[149] *Id.* at 558.

[150] *Id.* at 559.

that the NYPD's widespread practices of heightening police enforcement on members of a racially defined group was unconstitutional.[151] Disappointingly, while there have been fewer stops since the court's decision, both the racial profiling of African Americans and Hispanic and the aggressive policing of minority communities continues.[152]

Notably, an especially illuminating aspect of Judge Scheindlin's decision was her discussion of the influence of unconscious racial bias, an issue not often mentioned in court opinions: "It would not be surprising if many police officers share the latent biases that pervade our society. If so, such biases could provide a further source of unreliability in officers' rapid, intuitive impressions of whether an individual's movements are furtive and indicate criminality."[153] Gray echoes that implicit bias played a major role in the NYPD's stop and frisk program—a program that provides "a snapshot of stop and frisk policies and practices across the country . . . ."[154] He reasons, "[I]mplicit bias probably accounts for much of the racial disparity in stop and frisk programs. As products of our society, officers just naturally look more closely at Black and Latinos citizens and are far more likely to attribute nefarious motives to them and their actions."[155]

B. Digital Surveillance Technology Policing 3.0 in a Post-September 11th World

The war on drugs got a shot in the arm with the "War on Terror." After the September 11th attacks on America, federal and local agencies began to work collaboratively under the auspices of fighting the war on terror. Soon after, the Bush Administration implemented policies allowing governmental agents to execute arbitrary searches of laptops, cameras, cell

---

[151] *Id.* at 562–63.

[152] *See* Jenn Rolnick Borchetta et al., Opinion, *Don't Let the Police Wreck Stop-and-Frisk Reforms*, N.Y. TIMES (Apr. 10, 2018), https://www.nytimes.com/2018/04/10/opinion/police-stop-and-frisk-reforms.html (analyzing the court ordered reform process for the NYPD to improve police discipline and supervision, and criticizing potential opposition by police needed reforms while advocating three reforms: (1) serious penalties for police misconduct; (2) issue of department smart phones for accurate note-keeping; and (3) the creation of a citywide community oversight board).

[153] *Floyd*, 959 F. Supp. 2d at 580–81.

[154] GRAY, *supra* note 3, at 53.

[155] *Id.* at 54.

phones, or other electronic devices at this nation's borders.[156] The umbrella of "national security" allows the government to obtain information about terror suspects from internet providers, phone companies, banks, and credit reporting agencies without any warrant.[157] Some of this aggressive policing, which Friedman calls "policing without permission," is misguided because it is executed largely in secret without oversight.[158] These tools and strategies used by the government threaten the Fourth Amendment's safeguards.[159] As a rejoinder, Friedman wants oversight over police conducting warrantless searches and discriminatory searches and proposes democratic policing of cops, which requires legislators, the police, and courts working together in collaborative reform efforts.[160]

Age of Surveillance and *Unwarranted* significantly overlap most in their exploration of how racial discriminatory policies are accomplished with technology. At a broad level, police departments across the country increasingly rely on predictive policing, a method of crime-mapping in which data about geographic areas is used to try to anticipate where crimes will happen.[161] Policing and investigations have been assisted by new data technologies, algorithms, digitized facial recognition technologies, social media scraping, data mining, person-based and place-based predictive analytics, and reliance on big data.[162] Big data is used to identify "predictive risk factors that correlate with criminal activity."[163]

---

[156] *See* Daniel Victor, *Forced Searches of Phones and Laptops at U.S. Border are Illegal, Lawsuit Claims*, N.Y. TIMES (Sept. 13, 2017), https://www.nytimes.com/2017/09/13/technology/aclu-border-patrol-lawsuit.html (indicating that the policy began under the Bush Administration).

[157] FRIEDMAN, *supra* note 8, at 292–96; *see also* Charlie Savage, *Congress Approves Six-Year Extension of Surveillance Law*, N.Y. TIMES, (Jan. 18, 2018), https://www.nytimes.com/2018/01/18/us/politics/surveillance-congress-snowden-privacy.html (reporting that the Senate voted to extend the National Security Agency's surveillance program allowing the warrantless collection of emails, texts, phone calls, and private messages from American companies, including AT&T and Google).

[158] FRIEDMAN, *supra* note 8, at 16–17, 20.

[159] *See id.* at 287.

[160] *See id.* at 316–22.

[161] *See* GRAY, *supra* note 3, at 38, 40, 264.

[162] *See* FERGUSON, *supra* note 142, at 2, 4; *see also* Taslitz, *supra* note 88, at 125 (describing use of facial recognition technology by Florida police to survey a downtown nightlife district).

[163] FERGUSON, *supra* note 142, at 167.

This is how race comes into play. Predictive analytics, social network theory, and data-mining technology appear race-neutral on the surface, but can be based on factors that correlate with race and class.[164] More narrowly, data-driven policing means aggressive police presence and surveillance, which manifests into harassment against African Americans, immigrants, religious groups, the poor, and protesters.[165] Residents in high crime areas who have frequent contact with police may be increasingly linked to others in the same situation, potentially leading to an endless loop of systematic bias by police associating individuals with their neighborhoods, family, or friends.[166] In the aggregate, this reveals the explicit and implicit bias of big data that is consistent with the racial history and systematic inequalities of American policing.[167]

Consider the ShotSpotter, a digital policing tool that is planted in high crime areas through strategically placed, networked, powerful acoustic sensors connected to GPS.[168] A ShotSpotter automatically identifies the sounds of gunshots to pinpoint an exact location and alert police to potential violent crime before it is reported by human witnesses; such devices have been deployed in high crime areas in Washington, D.C., Boston, Oakland, San Fransisco, San Antonio, and Minneapolis.[169] ShotSpotter sensors can also pick up outside conversations, sounds, and other audio without the consent and knowledge of individuals, which could be used in the prosecution's case.[170] Just like Stingrays, Shotspotters are a new technology that assists the government in sustaining the mass incarceration machinery.

---

[164] *See id.* at 103–04; *see also* Michelle Alexander, *The Newest Jim Crow*, N.Y. TIMES (Nov. 8, 2018), https://www.nytimes.com/2018/11/08/opinion/sunday/criminal-justice-reforms-race-technology.html.

[165] *See* FERGUSON, *supra* note 142, at 5.

[166] *Id.* at 56–57.

[167] *Id.* at 131–32.

[168] *See* SHOTSPOTTER, https://www.shotspotter.com (last visited Sept. 5, 2019).

[169] *Id.*; *see also* Dean Weingarten, *San Antonio Pulls the Plug on ShotSpotter Gunfire Detection System, Hartford, CT Next?*, THE TRUTH ABOUT GUNS (Aug. 21, 2017), http://www.thetruthaboutguns.com/2017/08/dean-weingarten/san-antonio-pulss-the-plug-on-shotspotter-gunfire-detection-system-hartford-ct-next/.

[170] *See* Suraj K. Sazawal, *Is ShotSpotter Violating Your Fourth Amendment Rights And You Don't Even Know?*, RIGHTS AND DISSENT (May 8, 2015), https://www.rightsanddissent.org/news/is-shotspotter-violating-your-fourth-amendment-rights-and-you-dont-even-know/.

IV. *UTAH V. STRIEFF*: ASSAULTING THE EXCLUSIONARY RULE AND ENABLING STINGRAY SURVEILLANCE

This section takes a procedural turn. As the Court pushes back against police encroachment on the constitutional rights of defendants in substantive Fourth Amendment surveillance cases, the Court is also simultaneously whittling away at the Fourth Amendment in its procedural rulings. For example, the police can stop any individual they want based on the suspicion that a crime is or was being committed. The Court's far-reaching ruling in *Utah v. Strieff* took a slice off of the Fourth Amendment exclusionary rule by allowing police officers to stop and question citizens based on a hunch or whim that a criminal violation has occurred.[171]

In *Strieff*, the Court ruled five to three in favor of the State of Utah and held that contraband obtained over the course of an illegal search did not violate Strieff's Fourth Amendment rights and as a result was not subject to suppression under the exclusionary rule.[172] A Utah narcotics detective engaged in a weeklong "intermittent" surveillance of a house based on an anonymous tip left on a drug tip line about "narcotics activity" at that specific house.[173] He observed a number of people making brief visits to the residence over the course of a week that made him suspicious that the occupants were dealing drugs.[174] Driving an unmarked car, the detective followed Strieff from the residence to a nearby lot and detained him, asking him what he was doing at the house.[175] After checking Strieff's identification through the police dispatcher, the detective learned of Strieff's

---

[171] Utah v. Strieff, 136 S. Ct. 2056, 2059 (2016); *id.* at 2064 (Sotomayor, J., dissenting). The exclusionary rule applies when there is a substantial causal connection between the illegal activity and the evidence offered at trial. *See* SALTZBURG & CAPRA, *supra* note 118, at 529. The Court has repeatedly declined to extend the exclusionary rule. *See* Herring v. United States, 555 U.S. 135, 137 (2009) (holding that the exclusionary rule does not apply when an isolated incident of police negligence leads to an unlawful search); Hudson v. Michigan, 547 U.S. 586, 586, 599 (2006) (declining to apply exclusionary rule to a knock-and-announce violation); *see also* David A. Moran, *The End of the Exclusionary Rule, Among Other Things: The Roberts Court Takes on the Fourth Amendment in the Fourth*, 2006 CATO SUP. CT. REV. 283, 301 (2006) (criticizing the Court for "completely recast[ing] the exclusionary rule as a narrow remedy that applies only when the evidence seized is of the type that the constitutional protection was designed to protect").

[172] 136 S. Ct. at 2064.

[173] *Id.* at 2059–60.

[174] *Id.* at 2057.

[175] *Id.*; State v. Strieff, 286 P.3d 317, 320 (Utah Ct. App. 2012), *rev'd*, 357 P.3d 532 (Utah 2015), *rev'd*, 136 S. Ct. 2056 (2016).

outstanding arrest warrant for an unpaid traffic ticket.[176] A baggie of methamphetamine and drug paraphernalia were found on Strieff during a search incident to arrest, and he was subsequently charged with unlawful possession of methamphetamine and drug paraphernalia.[177]

At the suppression hearing, the prosecutor responded to Strieff's claim that it was an unlawful investigatory stop, conceding that the officer lacked reasonable suspicion for stopping Strieff because the detective never saw Strieff enter the suspected drug house or knew how long Strieff was there.[178] The State argued however, that even though there was no reasonable suspicion for the stop, the valid arrest warrant attenuated the connection between the unlawful stop and the discovery of the contraband.[179]

The issue presented to the Court was whether the attenuation doctrine applies where an unconstitutional detention leads to the discovery of a valid arrest warrant.[180] Writing for the majority, Justice Thomas applied the *Brown v. Illinois*[181] three-factor test to determine if the exclusionary rule applied based on a substantial causal connection between the illegal activity and the evidence offered at trial or whether the evidence was sufficiently attenuated from the original warrant.[182] He concluded that: (1) "temporal proximity" between the initial unlawful stop and the search favors suppressing the evidence because the drugs were found on Strieff minutes after the stop; (2) the "presence of intervening circumstances" strongly favors the state because the valid warrant authorizing Strieff's arrest existed before his stop and was unrelated to the investigation of the suspected drug house; and (3) there was no misconduct because the officer only acted negligently, which did not rise to a "purposeful or flagrant" violation of Strieff's Fourth Amendment rights.[183] As Justice Thomas reasoned, "[T]here is no indication that this unlawful stop was part of any systemic or recurrent

---

[176] *Strieff*, 136 S. Ct. at 2060; State v. Strieff, 357 P.3d 532, 536 (Utah 2015), *rev'd*, 136 S. Ct. 2056 (2016).

[177] *Strieff*, 136 S. Ct. at 2060.

[178] State v. Strieff, 357 P.3d 532, 536–37 (Utah 2015), *rev'd*, 136 S. Ct. 2056 (2016).

[179] *Strieff*, 136 S. Ct. at 2060.

[180] *Id.*

[181] 422 U.S. 590 (1975).

[182] *Strieff*, 136 S. Ct. at 2061–62.

[183] *Id.* at 2062–63.

police misconduct . . . all the evidence suggests that the stop was an isolated instance of negligence that occurred in connection with a bonafide investigation of a suspected drug house."[184]

Perhaps to the chagrin of Justice Thomas, there is an alternative interpretation of the facts to support the conclusion that this was not a so-called "isolated instance of negligence." The remainder of this section offers a close reading of the majority opinion, reveals its flaws, and concludes that *Strieff* establishes a bad precedent that further empowers the great unfettered discretion officers already have. First, the centerpiece of the opinion's infirmities is Justice Thomas's misreading of *Brown*, a case wherein the suspect made two inculpatory statements after being arrested without probable cause and being given *Miranda* warnings twice.[185] At issue was whether a *Miranda* warning sufficiently breaks the causal chain between an illegal arrest and a confession.[186] The *Brown* Court held that there was no break because *Miranda* warnings, per se, cannot make the act of confession a product of free will sufficient enough to break the causal connection between the confession and the illegal arrest.[187] In comparison, there was no significant intervening event analyzed in *Strieff*. Attenuation from the discovery of the contraband came by the detective's exploitation of his own illegal conduct.[188]

Second, Justice Thomas erroneously construed the officer's conduct as not being "purposeful and flagrant" but as an "isolated instance of negligence."[189] To the contrary, the detective committed to a surveillance spanning a week, based not on a reliable informant's tip, but rather on an isolated anonymous tip left on a caller hotline.[190] As such, the stopping of Strieff was as purposeful as the actions of the Chicago police officers who broke into petitioner's apartment in *Brown*. There, the officers searched Brown's apartment and arrested him without probable cause or a warrant, in order to question him in an ongoing murder investigation.[191] As Justice Blackmun, writing for the

---

[184] *Id.* at 2063.

[185] *See Brown*, 422 U.S. at 594–96.

[186] *Id.* at 597.

[187] *Id.* at 603–04.

[188] *See Strieff*, 136 S. Ct. at 2064–65 (Sotomayor, J., dissenting) (describing how "[i]n his search for lawbreaking, the officer in this case himself broke the law").

[189] *Id.* at 2063–64.

[190] *Id.* at 2059–60.

[191] *See Brown*, 422 U.S. at 592.

majority in *Brown*, pointed out, "the illegality here . . . had a quality of purposefulness. The impropriety of the arrest was obvious; awareness of that fact was virtually conceded by the two detectives . . . . The arrest, both in design and execution, was investigatory."[192] Similarly, the same could be said of the detective's stopping of Strieff without reasonable suspicion; it was a stop simply made for the purpose of embarking on a fishing expedition, hoping to reel something in.

A fuller understanding is presented by Justice Sotomayor's dissent where she applied the same *Brown* factors to obtain an opposite result: the officer illegally stopped Strieff and discovered the drugs by "exploiting his own illegal conduct."[193] As to the first *Brown* factor, Justice Sotomayor astutely recognized that there was no time lapse since the officer performed a warrant check immediately after stopping Strieff.[194] Furthermore, there was no intervening circumstance because Salt Lake County's enormous backlog of outstanding warrants was well known to officers, and thus "the officer's discovery of a warrant was not some intervening surprise that he could not have anticipated."[195]

Next, Justice Thomas misinterpreted *Segura v. United States*[196] and again, erroneously relied on an inapposite case to support a contrary conclusion. Justice Kagan acknowledges as much in a footnote in her dissent in *Strieff*:

> [In *Segura*], [t]he Court . . . held that the Fourth Amendment violation at issue "did not contribute in any way" to the police's subsequent procurement of a warrant and discovery of

---

[192] *Id.* at 605.

[193] *Strieff*, 136 S. Ct. at 2066–67 (Sotomayor, J., dissenting).

[194] *Id.* at 2066.

[195] *Id.* at 2067. Orin Kerr also critiques the majority's use of the *Brown* factors. *See* Orin Kerr, *Opinion Analysis: The Exclusionary Rule is Weakened But It Still Lives*, SCOTUSBLOG (June 20, 2016, 9:35 PM), http://www.scotusblog.com/2016/06/opinion-analysis-the-exclusionary-rule-is-weakened-but-it-still-lives/. The *Brown* three-factor test, as used by Justice Thomas, is not a well settled doctrine as the majority portrays it to be. *Id.* Kerr theorizes that the Court in *Brown* did not apply a strict three factor test, but rather a totality-of-the-circumstances approach. *Id.* Moreover, he believes that an "intervening circumstance" should be considered "an outside event that changes what is expected to happen." *Id.* Thus, in *Strieff*, there was no intervening circumstance because the police stop went according to plan; an officer conducting a warrant check could expect a warrant to appear. Indeed, the "existence of the warrant is only an intervening circumstance if you didn't expect Strieff to have a warrant out for his arrest." *Id.* Finally, under the third *Brown* factor, the burden of proof in establishing attenuation is on the government. *Id.*

[196] 468 U.S. 796 (1984).

> contraband. So the Court had no occasion to consider the question here: What happens when an unconstitutional act in fact leads to a warrant which then leads to evidence?[197]

In extrapolating Justice Kagan's footnote further, *Segura* appears to have relied on the independent source doctrine. Specifically, the Court in *Segura* considered whether to supress evidence procured during an illegal search when officers later obtained a warrant predicated on probable cause free of the information from the intital search.[198] New York Drug Enforcement Task Force agents relied on a tip and conducted weeks-long surveillance over Segura's apartment.[199] They were instructed to "secure" the premises to prevent the destruction of evidence.[200] Alarmingly, law enforcement agents forcibly entered Segura's apartment, without requesting or receiving permission.[201] In dissent, Justice Stevens referred to the day-long police occupation of Segura's apartment and surmised that these facts epitomized the deterrence rationale behind the exclusionary rule, and thus the evidence obtained should have been excluded.[202] The *Segura* Court declined to suppress the evidence because "the illegal entry into petitioners' apartment did not contribute in any way to discovery of the evidence seized under the warrant."[203]

In contrast, the officer's illegal conduct in *Strieff* did actually contribute to the discovery of the evidence procured in the search.[204] Justice Sotomayor explained that the facts of the two cases are markedly distinguishable:

---

[197] *Strieff*, 136 S. Ct. at 2073 n.2 (Kagan, J., dissenting) (citing *Segura*, 468 U.S. at 815).

[198] *See Segura*, 468 U.S. at 797–98.

[199] *Id.* at 799–800. Bearing this in mind, Professor Joshua Dressler referred to *Segura* decades earlier as a hurried, "inherently flawed," and "unnecessarily weak" decision. *See* Joshua Dressler, *A Lesson in Caution, Overwork, and Fatigue: The Judicial Miscraftsmanship of* Segura v. United States, 26 WM. & MARY L. REV. 375, 410–11 (1985). According to Dressler, that opinion authored by Chief Justice Burger offered reasoning and a conclusion based only on implied legal authority pulled from prior Court cases that were factually distinguishable. *Id.* at 405–07. Dressler asserts that the case is the wrong precedent for addressing the issue of securing premises in the absence of exigent circumstances. *Id.* at 411.

[200] *Segura*, 468 U.S. at 800.

[201] *Id.*

[202] *Id.* at 836–38 (Stevens, J., dissenting).

[203] *Id.* at 815 (majority opinion).

[204] Utah v. Strieff, 136 S. Ct. 2056, 2067 (2016) (Sotomayor, J., dissenting).

> [I]t is difficult to understand [the majority's] interpretation. In *Segura*, the agents' illegal conduct in entering the apartment had nothing to do with procurement of a search warrant. Here, the officer's illegal conduct in stopping Strieff was essential to his discovery of an arrest warrant. *Segura* would be similar only if the agents used information they illegally obtained from the apartment to procure a search warrant or discover an arrest warrant.[205]

It is worth noting that Justice Sotomayor is the only Justice who mentioned *Wong Sun v. United States*[206]—the seminal "fruit of a poisonous tree" case—when she explained that the guiding principle of *Wong Sun* applied because that case turned on the fact that police officers exploited their initial illegal search to obtain tainted evidence.[207] According to Justice Sotomayor, "*Wong Sun* explains why Strieff's drugs must be excluded. We reasoned that a Fourth Amendment violation may not color every investigation that follows but it certainly strains the actions of officers who exploit the infraction. We distinguished evidence obtained by innocuous means from evidence obtained by exploiting misconduct."[208]

Taking Justice Sotomayor's cue, *Wong Sun*'s applicability does deserve more attention. *Wong Sun*'s analysis should have been used to resolve the issues in *Strieff*. At issue in *Wong Sun* was whether the illegality of the evidence to which an instant objection was made came about because of the illegality itself or instead by means sufficiently distinguishable to be purged of the primary taint.[209] The *Wong Sun* Court held that the narcotics clearly came about from the exploitation of illegality, and thus the statement made from an unlawful arrest may not be used.[210]

---

[205] *Id.*

[206] 371 U.S. 471 (1963).

[207] *See Strieff*, 136 S. Ct. at 2066 (Sotomayor, J., dissenting). *Wong Sun* centered on a series of warrantless drug busts in San Francisco involving Chinese American defendants and Chinese American narcotics agents working undercover. *Wong Sun*, 371 U.S. at 472–76. Based on a tip that Wah Toy and Wong Sun entered into a drug agreement to buy heroin, agents arrived at a laundry without obtaining an arrest warrant. *Id.* After obtaining information from Wah Toy, the agents executed two additional warrantless searches and only one of the searches turned up heroin. *Id.* In addition to finding the heroin inadmissible because of its relationship to unlawfully obtained tainted information, the Court for the first time applied the "fruits of the poisonous tree" doctrine to exclude verbal statements. *Id.* at 487–88, 492.

[208] *Strieff*, 136 S. Ct. at 2066 (Sotomayor, J., dissenting).

[209] *See generally Wong Sun*, 371 U.S. 471.

[210] *Id.* at 492.

There are striking similarities between *Wong Sun* and *Strieff*. The officers in *Wong Sun* wanted to make drug busts without having to secure proper search warrants. They were aware of what they were doing and acted intentionally in searching the laundromat and residences. Their misconduct was punished in the case because the evidence was excluded against one of Wong Sun's co-defendants.[211] With that in mind, Strieff's exploitation was more like that in *Wong Sun* than that in *Segura* because the officer in *Strieff* wanted to make a drug bust without a warrant and intentionally stopped Strieff in the hopes that he possessed contraband and had an outstanding warrant for his arrest. The officers however were not punished for this misconduct, and the evidence was admitted into evidence just because of the active warrant.

Yet incredibly, Justice Thomas disregards these key differences and states that "the Court addressed *similar facts to those here* and found sufficient intervening circumstances to allow the admission of evidence."[212] Justice Thomas surmised that the agents in *Segura* had probable cause to believe there was drug dealing in the apartment and sought a warrant which was not issued until the next day.[213] With the warrant pending, the agents entered the apartment, arrested an occupant, and then discovered evidence of drug activity.[214] Based on this shaky premise, Justice Thomas asserted that *Segura*'s principles apply in *Strieff* because in both cases, the connection between the unlawful conduct and the discovery of evidence was "sufficiently attenuated to dissipate the taint."[215]

Third, *Strieff* ignores the primary purpose of the exclusionary rule: the deterrence of unlawful police misconduct. Facing this contradictory evidence, how could the majority find that the officer acted in good faith? [216] Justice Kagan emphasized this irreconcilable fact in her conclusion:

> The majority chalks up Fackrell's Fourth Amendment violation to a couple of innocent "mistakes." But far from a Barney Fife-type mishap, Fackrell's seizure of Strieff was a calculated decision, taken with so little justification that the State has

---

[211] *Id.* The Court concluded that Wong Sun lacked standing to object because his Fourth Amendment rights were not violated. *Id.*

[212] *Strieff*, 136 S. Ct. at 2062 (emphasis added).

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] *Id.* at 2063.

> never tried to defend its legality. At the suppression hearing, Fackrell acknowledged that the stop was designed for investigatory purposes—i.e., to "find out what was going on [in] the house" he had been watching, and to figure out "what [Strieff] was doing there."[217]

The majority's good faith contention is further skewered in Justice Sotomayor's dissent, where she responded to the core deficiencies in the Court's analysis: "The officer found the drugs only after learning of Strieff's traffic violation; and he learned of Strieff's traffic violation only because he unlawfully stopped Strieff to check his driver's license." [218]

Strieff allows officers to retroactively claim grounds for making an unconstitutional stop and circumvent the exclusionary rule. In essence, *Strieff* allows police officers to stop people to check for warrants, regardless of any belief of wrongdoing.[219] Stephen Saltzburg contends, "[*Strieff*'s] practical effect might be to greatly enhance law enforcement incentives to make 'stops' without the necessary reasonable suspicion and might affect a large number of people." [220] Put simply, if there is no warrant, the suspect will be allowed to leave. If there is a warrant, he can be searched incident to arrest and questioned further.

This issue can arise in a Stingray surveillance case. *Patrick*, discussed earlier in Part II, is a case on point. There, the Seventh Circuit broadly interpreted *Strieff* as precluding the application of the exclusionary rule.[221] However, in her dissent, Judge Wood argued that the panel majority unnecessarily extended *Strieff* by failing to see that the facts were distinguishable; the police got the arrest warrant, used the Stingray to locate Patrick, and then found the gun in plain view

---

[217] *Id.* at 2072 (Kagan, J., dissenting) (citations omitted).

[218] *Id.* at 2066 (Sotomayor, J., dissenting).

[219] *See* Ronald C. Tyler, Utah v. Strieff*: A Bad Decision on Policing With a Gripping Dissent by Justice Sotomayor*, STAN. L. SCH. BLOGS (July 5, 2016), https://law.stanford.edu/2016/07/05/utah-v-strieff-a-bad-decision-on-policing-with-a-gripping-dissent-by-justice-sotomayor/; Editorial Board, *Another Hit to the Fourth Amendment*, N.Y. TIMES (June 20, 2016), https://www.nytimes.com/2016/06/21/opinion/another-hit-to-the-fourth-amendment.html.

[220] *See* Stephen Salzburg, Response, Utah v. Strieff*: Chipping Away at the Exclusionary Rule*, GEO. WASH. L. REV. ON THE DOCKET (June 23, 2016), https://www.gwlr.org/utah-v-strieff-chipping-away-at-the-exclusionary-rule/.

[221] United States v. Patrick, 842 F.3d. 540, 542 (7th Cir. 2016); *id.* at 549 (Wood, J., dissenting).

during the arrest.[222] From her point of view, the arrest warrant was not an intervening cause and could not have attenuated any potential taint.[223]

Lastly, while the *Strieff* majority opinion did not mention it, the decision will have far-reaching effects on minority communities. Citing to social science studies outside of the record about the influence of race on criminal procedure, including Alexander's work on mass incarceration, Justice Sotomayor was the only Justice to acknowledge the racial realities of American society.[224] She made insightful points about the majority opinion, finding that the *Strieff* ruling "allows the police to stop you on the street, demand your identification, and check it for outstanding traffic warrants—even if you are not doing anything wrong," [225] enabling officers to arbitrarily target citizens and racial minorities who are disproportionately impacted.[226] As discussed throughout this Review, this is just the kind of twenty-first century policing that Gray and Friedman vehemently oppose and warn readers about.

V. GPS MONITORING AND SUPERVISED PROBATION IN WASHINGTON, D.C.

This closing section discusses the unfettered discretion exercised by the MPD when embarking on indiscriminate searches using Veritrax GPS records to look for potential suspects who may be on supervised probation. This issue has received scant attention because the increase in the number of people on community supervision, or "mass supervision" through probation and parole, is largely not given the attention that it deserves.[227]

Akin to mass incarceration, supervised release also reflects racial inequality: African Americans make up thirty percent of those on probation or parole, most of whom were convicted of

---

[222] *Id.* at 549–50.

[223] *Id.* at 550.

[224] *See* Utah v. Strieff, 136 S. Ct. 2056, 2070–71 (2016) (Sotomayor, J., dissenting).

[225] *Id.* at 2064.

[226] *Id.* at 2070–71.

[227] *See* PEW CHARITABLE TRUSTS, PROBATION AND PAROLE SYSTEMS MARKED BY HIGH STAKES, MISSED OPPORTUNITIES 4 (Sept. 25, 2018), https://www.pewtrusts.org/-/media/assets/2018/09/probation_and_parole_systems_marked_by_high_stakes_missed_opportunities_pew.pdf.

drug and property crimes.[228] Because they are subject to postconviction surveillance and court ordered rules, a third of them will likely return to jail or prison for violating a myriad of rules, including prohibitions on drug and alcohol use, having contact with felons, failing to pay fines and fees, and disobeying movement restrictions.[229] A person on supervision in Washington, D.C. is especially vulnerable to searches, because unlike other jurisdictions, Washington, D.C. has no search condition statute that puts supervisees on notice, and the only warning provided is the ostensibly benign advisal that the supervisees' "movement will be tracked and stored as an official record."[230] Plus, GPS monitoring is far more intrusive than a search of a person or home because the MPD have real-time, direct access to a database with up to twenty years of data.[231]

The MPD's practice of circumventing the Fourth Amendment by running random searches of the supervision data, and importing specific names of supervisees to lock in their location, stands at the new frontier of Fourth Amendment litigation. The Public Defender Service successfully litigated this very issue in *United States v. Jackson,* where the Superior Court of D.C. held that the MPD violated Jackson's Fourth Amendment rights when it unlawfully searched Jackson's GPS location information without suspicion and absent any probation violation.[232] The MPD accessed Jackson's GPS location information, maintained pursuant to a GPS contract executed between Jackson and the Court Services and Offender Supervision Agency ("CSOSA"), during their investigation of an armed robbery by two unknown African American men.[233] Without specifically identifying Jackson, or even having witness accounts of seeing one of the men wearing a GPS monitoring device, the MPD looked for

---

[228] *Id.* at 7.

[229] *See id.* at 9; Michelle Suzanne Phelps, *Why Ending Mass Probation is Crucial to Criminal Justice Reform*, SCHOLARS STRATEGY NETWORK (Sept. 14, 2018), https://scholars.org/brief/why-ending-mass-probation-crucial-us-criminal-justice-reform.

[230] Reply to Government's Opposition to Defendant's Supplemental Motion to Suppress Tangible Evidence and Electronic Data at 7, United States v. Jackson, No. 2015 CFS 2512 (D.C. Super. Ct. March 11, 2016) (on file with the author).

[231] Court Services and Offender Supervision Agency for the District of Columbia, 71 Fed. Reg. 15177, 15178 (Mar. 27, 2006).

[232] Order Granting Defendant's Supplemental Motion to Suppress Tangible Evidence and Electronic Data at 21, *Jackson*, No. 2015 CFS 2512 (on file with the author).

[233] *Id.* at 1.

anyone wearing a GPS monitor near the crime scene.[234] The MPD eventually captured GPS records showing all of Jackson's movements over multiple weeks, including movements in Jackson's private home.[235] These records were used to track down Jackson and another man at their home, which lead to the finding of a black ski mask and an SUV that was tied to the robbery.[236]

At the suppression hearing, the Government argued that Jackson consented to be placed on probation, and thus consented to the police searching his location data; he had no legitimate expectation of privacy.[237] The Government also asserted that the "special needs" exception to the Fourth Amendment allows searches conducted without any ground for suspicion of particular individuals in certain limited circumstances,[238] and thus the search was authorized. Defense counsel argued that the search of Jackson's GPS location information was a "fishing expedition" done for law enforcement purposes.[239] They stated that though Jackson was placed on GPS supervision by CSOSA

---

[234] *Id.* at 2.

[235] *Id.*

[236] *Id.*

[237] Reply to Government's Opposition to Defendant's Supplemental Motion to Suppress Tangible Evidence and Electronic Data, *supra* note 230, at 1–2.

[238] Order Granting Defendant's Supplemental Motion to Suppress Tangible Evidence and Electronic Data, *supra* note 232, at 14. Supreme Court precedent allows for GPS monitoring: "A State's operation of a probation system, like its operation of a school, government office, or prison, or its supervision of a regulated industry, likewise presents 'special needs' beyond normal law enforcement that may justify departures from the usual warrant and probable-cause requirements." Griffin v. Wisconsin, 483 U.S. 868, 873–74 (1987). This "special needs" rationale is discarded for a generic balancing test when the searching party is not a probation officer, but a police officer. United States v. Knights, 534 U.S. 112, 118–19 (2001) ("[W]e conclude that the search of Knights was reasonable under our general Fourth Amendment approach of 'examining the totality of the circumstances.' " (quoting Ohio v. Robinette, 519 U.S. 33, 39 (1996))). "The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which is needed for the promotion of legitimate governmental interests.' " *Knights*, 534 U.S. at 118–19 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[239] Reply to Government's Opposition to Defendant's Supplemental Motion to Suppress Tangible Evidence and Electronic Data, *supra* note 230, at 10.

to track his whereabouts, that fact does not make it less of a search, and that search must also be reasonable.[240] Defense counsel contended that:

> CSOSA completely frustrated the purpose of the Privacy Act . . . by granting MPD unfettered access to its GPS database. MPD did not follow the Code's procedure . . . . Instead, MPD ran a general search into a CSOSA's database, without any information as to whether anyone placed on electronic monitoring was a suspect of the offense.[241]

CONCLUSION

In the end, *Age of Surveillance* and *Unwarranted* are terrific books that reveal the lack of clarity in current Fourth Amendment jurisprudence as it relates to emerging technologies. The idealistic authors successfully present a prescription on how to nurse an ailing Fourth Amendment jurisprudence. Gray argues that the text and history of the Fourth Amendment provide effective constitutional remedies and would be effective in meeting contemporary threats if they are taken seriously by courts and law enforcement agencies. Along a similar line, Friedman contends that the collective dimension of the Fourth Amendment should be taken seriously to ensure the collective security of the people. The burden now rests on the people to take action. We must demand more transparency of police surveillance and be allowed to participate in the decisionmaking process regarding how surveillance technology is used. We must also require more police accountability and better training for officers and judges so that they can understand the influence of the unconscious biases that we all have. Unquestionably, these goals must be met if we are to protect privacy rights and slow down the continual erosion of the Fourth Amendment.

---

[240] *See id.* at 9. In reversing the North Carolina Supreme Court's denial of a motions hearing, the Court stated, "the only theory we discern in that passage is that the State's system of nonconsensual satellite-based monitoring does not entail a search within the meaning of the Fourth Amendment. That theory is inconsistent with this Court's precedents." Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015) (per curiam).

[241] Reply to Government's Opposition to Defendant's Supplemental Motion to Suppress Tangible Evidence and Electronic Data, *supra* note 230, at 14.