BOOK REVIEW

Surveillance State: Fourth Amendment Law, Big Data Policing, and Facial Recognition Technology

Harvey Gee*

The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. Andrew Guthrie Ferguson. New York University Press, 2017. Pp.259. $28.00

Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century. Ric Simmons. Cambridge University Press, 2019. Pp.264. $34.99

DOI: https://doi.org/10.15779/Z38SJ19R9R.

*. 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. B.A., Sonoma State University; J.D., St. Mary's School of Law; LL.M., The George Washington Law School.

The author thanks the editors of the Berkeley Journal of African-American Law & Policy, including Nazeerah Ali, Aneil Dhillon, Adrianna Dinolfo, Clara Dorfman, Colleen Fitzgerrell, Tatiana Fominyam, Maya Harmon, Ben Holston, Flora Morgan, Jenna Mowat, Serena Nichols-Quintana, Knychelle Passmore, and Jimmy Sanders, for their helpful comments, suggestions, and overall hard work in preparing this review.

INTRODUCTION

The surveillance state is here. Law enforcement in major cities used surveillance technology to watch and track protesters in the mass protests over the deaths of George Floyd, Ahmaud Arbery, Breonna Taylor, Rayshard Brooks, and other young African Americans.[1] The Department of Homeland Security monitored and tracked Black Lives Matter (BLM) protests in more than 15 cities using military-grade technology, including infrared and electro-optical cameras and "dirty box" devices on airplanes, drones, and helicopters.[2] On the ground, the San Francisco Police Department conducted real-time mass video surveillance of BLM protesters despite a citywide ban on such conduct.[3] Such digital spying is not new. For the past decade, police departments across the country, in an effort to reduce gun violence, have been using ShotSpotter gunshot technology in minority communities to track the sound of gunshots.[4] In 2014, Stingrays were used as spying tools by local police departments during demonstrations.[5] And despite initial denials, the Los Angeles Police Department admitted to using facial recognition nearly 30,000 times since 2009.[6]

Do Fourth Amendment protections even exist in such public forums? Who decides the limits and efficacy of the police use of mass-surveillance

1. *See* Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES, June 19, 2020, https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.

2. *Id.*

3. *See* Dave Maass & Mathew Guariglia, *San Francisco Police Accessed Business District Camera Network to Spy on Protesters*, ELEC. FRONTIER FOUND., July 27, 2020, https://www.eff.org/deeplinks/2020/07/san-francisco-police-accessed-business-district-camera-network-spy-protestors.

4. *See* Elizabeth MacBride, *The Scientist, The Investor and The CEO: How 'Shots Fired!' Technology Turned a Profit*, FORBES, Oct. 30, 2018, https://www.forbes.com/sites/elizabethmacbride/2018/10/30/the-scientist-the-investor-and-the-ceo-how-shotspotter-turned-a-profit-after-22-years/.

5. See Kate Klonick, *Stingrays: Not Just For Feds! How Local Law Enforcement Uses an Invasive Unreliable Surveillance Tool*, SLATE, Nov. 10, 2014, https://slate.com/technology/2014/11/stingrays-imsi-catchers-how-local-law-enforcement-uses-an-invasive-surveillance-tool.html.

6. Hosted, AP, *Report: LAPD Used Facial Recognition Nearly 30,000 Times*, ASSOCIATED PRESS, Sept. 21, 2020, https://hosted.ap.org/article/b45a07e5430aa4565930d5e606788714/report-lapd-used-facial-recognition-nearly-30000-times.

technologies to monitor peaceful protests? Will the police continue to use these new technologies to disproportionately target racial minorities? Two books written by Fourth Amendment scholars attempt to unpack these questions. Readers in the pro-privacy rights and racial justice camps will resonate with Andrew Guthrie Ferguson in *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*.[7] Whereas readers who favor police using more law enforcement surveillance and investigation, and who disagree with the Supreme Court's recent Fourth Amendment technology rulings upholding the constitutional right to be protected from unreasonable searches and seizures by the government, will find Ric Simmons's *Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century* more appealing.[8]

Both books are persuasive and insightful. *Rise of Big Data Policing* and *Smart Surveillance* certainly add to the growing Fourth Amendment scholarship analyzing the impact of emerging surveillance technology on privacy.[9] Ferguson weighs the pros and cons of surveillance technology, and then dives deeper into its impact on racial communities. *Rise of Big Data Policing* consists of ten descriptive and prescriptive chapters covering the rise of data surveillance and data-driven policing, addressing the important questions of whom, where, when, and how we police. In contrast, *Smart Surveillance* enthusiastically embraces the view that more technology surveillance is needed because it can prevent crime, help catch criminals, monitor police, and reduce racial profiling. The eight chapters offer a cost-benefit analysis of surveillance and demonstrate how to measure the benefits of public surveillance, big data policing, and mosaic searches. The chapters conclude with a discussion of the third-party doctrine and

7. *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017). Ferguson teaches Criminal Law, Criminal Procedure, and Evidence at the University of the District of Columbia, David A. Clarke School of Law. Ferguson worked for the Public Defender Service in D.C. prior to his academic appointment.

8. *See* RIC SIMMONS, SMART SURVEILLANCE: HOW TO INTERPRET THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 144 (2019). Simmons is Chief Justice Thomas J. Moyer Professor for the Administration of Justice and Rule of Law, Moritz College of Law at The Ohio State University.

9. Ferguson and Simmons follow two other recent and worthwhile Fourth Amendment books. Barry Friedman's *Unwarranted: Policing Without Permission* explores why better police accountability is needed in a modern world. It is a critical dissection of the debates about policing, and a clarion call to take responsibility. Friedman says limitations must be placed on the unfettered discretion afforded to the police when they conduct traffic stops, stop-and-frisks, and use surveillance technology. *See* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION (Farrar et. al. eds., 2017). David Gray's *The Fourth Amendment in an Age of Surveillance* explains how the Fourth Amendment, though embattled, can have a prominent role in twenty-first century discussions of privacy, technology, and surveillance. *See* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017). He 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. I have comprehensively reviewed these works elsewhere. *See* Harvey Gee, *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*, 93 ST. JOHN'S L. REV. 325 (2019) (book review).

hyper-intrusive searches. Both books are timely, clearly written, and thoroughly researched.

This Review uses the dominant themes presented in *Rise of Big Data Policing* and *Smart Surveillance* to argue that the benefits of having public surveillance are significantly outweighed by the government's abuse of surveillance technology and the corresponding reduction in our reasonable expectation of privacy. Part One analyzes the primary arguments presented in *Rise of Big Data Policing*. Part Two considers the key arguments presented in *Smart Surveillance*. Part Three examines recent developments in surveillance technology and Fourth Amendment jurisprudence that have occurred since the release of the two volumes. This section builds on the substantive background provided by Ferguson and Simmons to extend the conversation about the inherent tensions between emerging surveillance and Fourth Amendment jurisprudence. Part Three focuses on some of the most popular and powerful surveillance tools used by local police departments with little oversight: pole cameras, Stingray cell-site simulators, and facial recognition and surveillance technology. These newer technologies purportedly help police fight crime, but they can also potentially infringe on privacy rights.

I. BIG DATA SURVEILLANCE, RACE, AND THE FOURTH AMENDMENT

A. Big Data Driven Policing, Race, and Terry v. Ohio

In *Rise of Big Data Policing*, Professor Ferguson explains how big data analyzes collected data and targets individuals by employing "person-based predictive targeting" and "place-based predictive targeting."[10] Person-based predictive policing uses data to identify and investigate potential criminal suspects.[11] Specifically, big data systems sift through criminal activity information to home in on the most violent and dangerous persons with an eye towards generating priority target lists.[12] Likewise, place-based predictive policing also uses a data-driven approach, relying on advanced data analytics to identify criminal patterns in specific geographic locations and deploy police resources.[13]

As with traditional policing, racial implications are unavoidable. This rise of predictive analytics, social network theory, and data-mining technology coincides with the need to respond to community outrage over the police killings of unarmed African Americans across the country.[14] On the one hand, police departments concerned with diminishing resources to patrol high-crime neighborhoods welcome new technology as enhanced and efficient policing

10. *See* FERGUSON, *supra* note 7, at 62.
11. *Id.* at 35.
12. *Id.* at 46.
13. *Id.* at 62.
14. *Id.* at 4.

tools.[15] On the other, Ferguson cautions that big data-driven policing often results in an aggressive police presence, surveillance, and harassment in communities of color.[16] Big data targeting can also distort and lower the reasonable suspicion requirement for stop-and-frisks for reasons correlated with race and class.[17] This creates a never-ending circle of racial profiling, whereby the police, fueled by suspicion, use specific personal information to make inferences about community residents.[18] Ferguson says that such a correlation could actually be tenuous and obfuscate environmental factors like neighborhood, family, or friend groups.[19] Therefore, the inputs and outputs of big data policing must be monitored for a disparate impact on communities of color.

Ferguson notes the origins of the modern police practice of targeting African Americans in the Supreme Court's landmark decision *Terry v. Ohio*.[20] There, Cleveland Police Detective Martin McFadden, who was in plain clothes, saw John Terry and Richard Chilton standing in front of a store window.[21] Terry and Chilton then walked and turned back to look at the same window.[22] A third man, Carl Katz, approached, briefly spoke with the two men, and then left.[23] McFadden suspected that the men were "casing" the store and engaged them.[24] McFadden grabbed Terry and spun him around so that he faced the other two men and patted down the outside of his clothes, including his overcoat.[25] McFadden felt a pistol in Terry's overcoat.[26] McFadden also patted down Chilton's outer clothing and found a revolver in his outer pocket.[27] Both men were charged with carrying a concealed weapon.[28]

Unmistakably, racism and brutality aimed at African Americans and patterns of a racially discriminatory policing policy lie at the heart of Ferguson's analysis.[29] Ferguson offers concrete examples. There was the 2014 shooting death of Michael Brown in Ferguson, Missouri which sparked awareness and protests bringing attention to the nationwide problem of police violence.[30] The author also discusses the federal lawsuit over "stop and frisk" practices in *Floyd v. City of N.Y.*,[31] which culminated in Judge Shira Scheindlin's finding that the

15. *Id.* at 28–29.
16. *Id*.
17. *Id*. at 57
18. *Id.*
19. *Id.* at 56–57.
20. 392 U.S. 1 (1968).
21. *Id.* at 6.
22. *Id.*
23. *Id.* at 6–7.
24. *Id.*
25. *Id.* at 7.
26. *Id.*
27. *Id.*
28. *Id.*
29. *See* FERGUSON, *supra* note 7, at 31.
30. *Id.* at 24, 31.
31. Floyd v. City of N.Y., 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

New York Police Department's proactive stop-and-frisk practices significantly targeted African Americans and Latinos in over 4 million stops between January 2004 and June 2012. This practice was held to be unconstitutional in 2013.[32] Unfortunately, in the years following *Floyd*, the racial profiling of African Americans and Latinos and aggressive policing continued in New York City's minority communities.[33]

The continuous calls for criminal justice reform, surging with the massive protests and worldwide outcry over George Floyd's death on May 25, 2020, support Ferguson's points about the unrelenting brutality invoked by the police against racial minorities. The brutality against Floyd, a 46-year-old African American, began after a convenience store employee called 911 to report that Floyd bought cigarettes with a counterfeit $20 bill.[34] The officers approached Floyd sitting in the driver's seat of an SUV.[35] Without explaining the reason for the stop, Officer Thomas Lane drew his gun and ordered Floyd to raise his hands.[36] Floyd was pulled out from the car and when the officers tried to forcibly place him into a squad car, Floyd resisted because he felt claustrophobic, and laid on the ground instead.[37] Officer Derek Chauvin, who is white, knelt on Floyd's neck for over 8 minutes as a pained and distressed Floyd begged "I can't breathe" more than 15 times before passing out.[38] Officer J. Alexander Kueng kneeled on Floyd's upper legs and held his wrists, as Officer Lane also held Floyd's legs, and Officer Tou Thao kept bystanders at a distance. After being fired from their jobs, Chauvin faced charges of murder and manslaughter while the other three officers were charged with manslaughter and aiding and abetting the murder.[39] A Minneapolis jury convicted Chauvin of second-degree

32. *See id.* at 556, 667.

33. *See* Jenn Rolnick Borchetta, et al., *Don't Wreck Stop-and-Frisk Reforms*, N.Y. TIMES, Apr. 1, 2018, https://www.nytimes.com/2018/04/10/opinion/police-stop-and-frisk-reforms.html (analyzing the court-ordered reform process for the New York Police Department to improve police discipline and supervision, and criticizing potential opposition by police while advocating three reforms: serious penalties for police misconduct, use of smart phones, and the creation of a citywide community oversight board).

34. *See* Evan Hill, et. al., *How George Floyd Was Killed in Police Custody*, N.Y. TIMES, May 31, 2020, https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html.

35. *George Floyd: What happened in the final moments of his* life, BBC NEWS, July 16, 2020, https://www.bbc.com/news/world-us-canada-52861726#:~:text=George%20Floyd%20dies%20after%20being,pronounced%20dead%20later%20in%20hospital.

36. *See Editorial, What to Know About the Death of George Floyd in Minneapolis*, N.Y. TIMES, Feb. 23, 2021, https://www.nytimes.com/article/george-floyd.html.

37. *Id.*

38. *See also* Evan Hill, et. al., *How George Floyd Was Killed in Police Custody*, N.Y. TIMES, May 31, 2020, https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html; George Floyd: *What Happened in the Final Moments of his Life*, BBC News, July 16, 2020, https://www.bbc.com/news/world-us-canada-52861726#:~:text=George%20Floyd%20dies%20after%20being,pronounced%20dead%20later%20in%20hospital.

39. *See* Editorial, *What to Know About the Death of George Floyd in Minneapolis*, N.Y. TIMES, Feb. 23, 2021, https://www.nytimes.com/article/george-floyd.html.

unintentional murder, third-degree murder, and second-degree manslaughter on April 20, 2021.[40]

During racial justice protests that followed Floyd's murder, the spotlight on the NYPD intensified again when New York Attorney General Letitia James filed a lawsuit against the NYPD in federal court alleging excessive force during the arrests of New Yorkers.[41] The complaint alleges that NYPD officers effectuated mass arrests without probable cause, unjustifiably deployed pepper spray, batons, and other force against protesters, and infringed upon the protesters' First Amendment rights.[42] These unlawful arrests, which also netted legal observers, medics, and other workers performing essential services, were made without probable cause.[43] The lawsuit seeks the implementation of an independent monitor to oversee NYPD policing tactics as well as broad injunctive relief, including systematic reforms to the NYPD's decades-long excessive force and false arrest practices. [44]

Next, Ferguson explains that the heavy policing in targeted areas of a city triggers racial justice concerns because of the large number of crimes occurring in poor minority neighborhoods and the implicit biases of police officers.[45] According to Ferguson, "This implicit bias shapes the raw information entering predictive systems, which in turn determines who gets targeted."[46] *Terry* is central to Ferguson's analysis since he considers it a representative example of small data policing.[47]

Even though Ferguson skips this fact, it is worth discussing how the Court ignored the racial dimensions of *Terry v. Ohio* by removing all references to race in its opinion. Ironically, *Terry* became one of the most important rulings with a

40. Amy Forlti, Steve Karnowski, & Tammy Webber, *Chauvin guilty of murder and manslaughter in Floyd's death*, AP, Apr. 20, 2021, https://apnews.com/article/derek-chauvin-trial-live-updates-04-20-2021-955a78df9a7a51835ad63afb8ce9b5c1. Weeks later, a federal grand jury indicated Derek Chauvin, Tou Thao, J. Alexander Kueng, and Thomas Lane on charges of violating George Floyd's civil rights during the arrest that led to his death. See Pete Williams & David K. Li, *Derek Chauvin, Three Other Ex-Minneapolis Police Officers Indicted by Federal Grand Jury*, NBC NEWS, May 7, 2021, https://www.nbcnews.com/news/us-news/derek-chauvin-three-other-ex-minneapolis-police-officers-indicted-federal-n1266671.

41. *See* Attorney General James Files Lawsuit Against the NYPD for Excessive Use of Force, Jan. 14, 2021, https://ag.ny.gov/press-release/2021/attorney-general-james-files-lawsuit-against-nypd-excessive-use-force. The genesis for the suit was Governor Cuomo's call for a civil investigation into police misconduct after videos circulated showing violent confrontations between apparently peaceful demonstrates and law enforcement. The Attorney General's office received more than 1,300 complaints and more than 300 written statements, and a three-day public hearing was held. Id. *See also* Erin Durkin, *New York Attorney General Suing NYPD Over Protest Response*, Politico, Jan. 14, 2021, https://www.politico.com/news/2021/01/14/new-york-attorney-general-suing-nypd-over-protest-response-459421.

42. Attorney General James Files Lawsuit Against the NYPD for Excessive Use of Force, *supra* note 41.

43. *Id.*

44. *Id.*

45. *See* FERGUSON, *supra* note 7, at 47.

46. *Id.* at 49.

47. *See id.* at 54–56.

racial impact.[48] Tracy Maclin insists this omission was regrettable because race may have influenced Officer McFadden's attitude toward the encounter.[49] Two of the suspects, Terry and Chilton, were Black, while Katz, the other suspect, was white.[50] In addition, the opinion failed to situate the case in its historical context by neglecting to mention the turbulent state of race relations and the increasing crime rate in the 1960s, or even noting what kind of store was surveyed by the men or details about the neighborhood.[51] Anthony Thompson, another scholar, explains that without any reference to race in *Terry*, no one would see the case as implicating racially motivated searches and seizures.[52] When race is injected back into the Court's statement of facts, the case was about a white detective noticing and watching two Black men standing on a street corner.[53] Thompson asserts, "The Court stripped away the racial dimension of the case by removing all racial references to the participant's race to manifest a forced officer-as-expert narrative."[54] Not surprisingly, to the casual observer the case was only about the totality of the circumstances.

The ruling was made at a time when probable cause was assumed to be the standard for all searches. Chief Justice Earl Warren, writing for the majority, analyzed this narrow question only: "whether it is always unreasonable for a policeman to seize a person and subject him to a limited search for weapons unless there is probable cause for an arrest."[55] They ruled that it was not.[56] The Court reasoned that there was no Fourth Amendment violation because McFadden's actions were consistent with his theory that the men were planning a daylight robbery, and it comported with the "reasonable suspicion" standard.[57]

Under *Terry,* police may stop a person if they have a reasonable suspicion that the person has committed or is about to commit a crime, and may frisk the suspect for weapons if they have reasonable suspicion that the suspect is armed and dangerous without violating the Fourth Amendment prohibition on unreasonable searches and seizures.[58] In practice, officers must point to some

48. *See* Hon. Jack B. Weinstein & Mae C. Quinn, *Terry, Race and Judicial Integrity: The Court and Suppression During the War on Drugs*, 72 ST. JOHN'S L. REV. 1323, 1329 (1998) (noting "[t]he *Terry* opinion did not mention the race of the men stopped for standing outside of the store, nor the race of the seizing officer.").

49. *See* Tracey Maclin, *"Black and Blue Encounters"—Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?*, 26 VAL. U. L. REV. 243, 267–68 (1991).

50. *See* Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 966–67 (1999).

51. *Id.*

52. *Id.* at 963.

53. *Id*. at 966.

54. *Id*. at 971 ("Terry essentially created a conceptual construct: an officer who was unaffected by considerations of race and who could be trusted even in a race-laden case like Terry to be acting on the basis of legitimate indicia of criminal activity.").

55. 392 U.S. at 15.

56. *Id.*

57. *Id*. at 27.

58. *Id*. at 29–30. Aware that future cases will present varying facts the Court professed: "We merely hold today that where a police officer observes unusual conduct which leads him

objective facts or observations that are sufficient to show reasonable suspicion in the circumstance, and afterwards, courts assess the reasonableness of searches and seizures from an objective point of view.[59] Officers have broad and completely unfettered discretion to conduct searches and seizures since the requirement to demonstrate reasonable suspicion of criminal wrongdoing has diluted so much since *Terry*.[60] The police can justify their decision to stop-and-frisk regardless of the true motivation, and courts tend to give them the benefit of the doubt.[61]

Regrettably, as search and seizure law developed, *Terry*'s "reasonable articulable suspicion" standard has been used as a weapon against minority communities during the race-based policing of the "War on Drugs".[62] Paul Butler explains how easy it is to meet the "reasonable suspicion" standard due to the standard set by *Terry*. Stop-and-frisk is the leading crime policy that allows African-American and Latino men to be stopped and frisked for trivial offenses like jaywalking or spitting on the sidewalk.[63] Similarly, from Devon Carbado's vantage point, *Terry* allows officers to use the reasonable suspicion excuse to stop-and-question people without any concern for officer or public safety.[64] More precisely, *Terry* enables "wholesale harassment" of African Americans through "prophylactic racial profiling" where the police officers aggressively target African Americans to deter them from possessing weapons or engaging in crime, without any belief that any evidence of criminality will be found.[65]

At the same time, *Terry* has defenders—Stephen Saltzburg argues that although the *Terry* opinion failed to carve out a clear rule for law enforcement, subsequent court interpretations have developed a workable standard that is logical and defensible in its application.[66] Likewise, Christopher Slobogin

---

reasonably to conclude in light of his experience that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous where in the course of investigating this behavior. . . makes reasonable inquiries, and where nothing in the initial stages of the encounter. . . dispel his reasonable fear for his own or other's safety he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons . . . ." *Id*. at 30.

59. Professor Stephen Saltzburg explains, "the [*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." *See* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, American Criminal Procedure: Cases and Commentary 201 (9th Ed. 2007).

60. Maclin, *supra* note 49, at 268.

61. *See* GRAY, *supra* note 9, at 279.

62. *See* Weinstein & Quinn, *supra* note 48, at 1323–1329.

63. *See* PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN 83, 115 (2017).

64. *See* Devon Carbado, *From Stop and Frisk to Shoot and Kill: Terry v. Ohio's Pathway to Police Violence*, 64 UCLA L. REV. 1508, 1521 (2017).

65. *Id.* at 1537.

66. *See* Stephen A. Saltzburg, *Terry v, Ohio: A Practically Perfect Doctrine*, 72 ST. JOHN'S L. REV. 911, 912 (2012); *see e.g.*, People v. Sibon, 219 N.E. 2d 1966, rev'd, 392 U.S. 40 (1968); Wainwright v. New Orleans, 392 U.S. 598 (1968); Adams v. Williams, 407 U.S. 143 (1972); Almeida-Sanchez v. United States, 413 U.S. 266 (1973); United States v. Brigoni-Ponce, 422 U.S. 873 (1975); New York v. Earl*, 431 U.S. 943* (1977); Ybarra v. Illinois, 444 U.S. 85 (1979);

agrees with *Terry's* proportionality principle, and he attributes criticisms of *Terry* to the inconsistent application of *Terry* in subsequent generations of litigation, which caused less individual privacy and more racial tensions in law enforcement.[67]

In the digital era, Ferguson conveys his fears that the application of big data information can dilute constitutional doctrines like reasonable suspicion by exploring a fictional *Terry* scenario where Terry had been identified by a big data algorithm as one of the top potential offenders in the city.[68] McFadden's testimony would be bolstered considerably, and the justification for the stop would be easier.[69] McFadden would testify about what he saw and about the reliability of "heat list" algorithms for officers, suspicion based on facial recognition software, and checks on police databases and social networking sites.[70]

Yet, the reliance on big data can also cut against the police. Here, Ferguson uses a Fourth Amendment suppression hearing to illustrate how data can be collected to determine which police officers were more accurate in stopping suspects.[71] At a hearing, data can be used to review the accuracy of an officer's prior success or failure in recovering contraband.[72] Data can show "how many times did the police officer get the question of suspicion 'wrong' before this particular correct stop." [73] Such a hit-rate pattern could affect officer credibility in court and influence how they conduct stop-and-frisks.[74]

Ferguson's lengthy coverage of the impact of surveillance technology on the constitutional rights of minority communities, a major strength of the book, extends to a discussion of what he calls "black data" which is big data policing based on erroneous algorithm correlations.[75] He asserts that black data is actually racially coded, because the data directly impacts communities of color.[76] Left unchecked, Ferguson contends that data-driven policing translates into aggressive police surveillance and harassment in communities of color. Sadly, as with protests arising from police killings of unarmed African Americans, the police can justify the ongoing targeting of poor communities in the name of using a "law and order" data-driven metric. Ferguson is especially skeptical of the way data-driven policing is championed as a way to ameliorate racially

---

Delaware v. Prouse, 440 U.S. 648 (1979); Dunaway v. New York, 442 U.S. 200 (1979); Brown v. Texas, 443 U.S. 47 (1979).

67. *See* Christopher Slobogin, *Let's Not Bury Terry: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1095 (1998).

68. *See* FERGUSON, *supra* note 7, at 55–56.

69. *Id.* at 56

70. *Id*. at 57.

71. *Id.* at 152–53.

72. *Id.* at 152.

73. *Id.*

74. *Id.* at 153.

75. *Id.* at 3–5.

76. *Id.* at 3.

discriminatory policing in a racially neutral manner.[77] He questions smart policing and data-driven policing because they have done little to alleviate longstanding "[f]ears of racial bias, a lack of transparency, data error," and the watering down of constitutional protections.[78] Ferguson asserts that new analysis will do little if the systematic racial biases remain in place.[79]

B. Real-Time Surveillance Tracking

Rise of Big Data Policing gains momentum with Ferguson's discussion of real-time surveillance and investigations when he explores new surveillance technologies influencing how and when police act.[80] Big data recording and listening, and tracking in real-time, allows for faster decision making because police have access to more information through data points than are available with traditional policing.[81] But, this pervasive surveillance also raises Fourth Amendment questions since new surveillance technologies alter traditional understandings of a reasonable expectation of privacy. Ferguson asserts, "Most modern police investigation takes advantage of this absence of constitutional protection from ordinary observational surveillance in public. The question becomes, does this analysis change with pervasive surveillance?"[82] He then elaborates on these points via a discussion of *United States v. Jones*,[83] where a unanimous Court expressed discomfort with the government's attachment of a global positioning system (GPS) tracker on a car for more than 28 days in a drug investigation, which was determined to be a "search."[84]

The *Jones* Court considered the general public's minimal expectations of privacy in public and the government's potentially invasive 24/7 surveillance tracking technologies.[85] Ferguson laments that the divergent opinions, though aware of the dangers of mass surveillance, offered no clear answer or guidance about emerging technologies.[86] Justice Scalia wrote the majority opinion concluding that the government's installation of a GPS device on defendant's jeep was a physical trespass, and thus a search under the Fourth Amendment.[87] The concurrences were concerned with long-term monitoring, which generates so much information about a suspect's movements and activities that the

77. *Id.* at 5.
78. *Id.* at 29.
79. *Id.* at 4–5.
80. *Id.* at 85.
81. *Id.* at 98.
82. *Id.*
83. 565 U.S. 400 (2012).
84. *See id.* at 403–408 (2012). Eleven years earlier, in *Kyllo v. U.S.*, 533 U.S. 27 (2001), the Court held that the use of a thermal imaging device (not in general public use) aimed at a private home from a public street to detect relative amounts of heat and obtain information about the interior of a home constitutes a "search" under the Fourth Amendment.
85. *See* FERGUSON, *supra* note 7, at 99.
86. *Id*. at 101.
87. *Jones*, 565 U.S. at 411.

aggregate effect is an invasion of privacy.[88] Justices Ginsburg, Breyer, Alito, and Kagan, in a separate concurrence, expressed overarching concerns about the impact of contemporary surveillance technologies on Fourth Amendment rights.[89] Justice Alito voiced concern over long-term surveillance and articulated that "the best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of deprivation of privacy that a reasonable person would not have anticipated."[90]

Justice Sotomayor wrote a separate concurrence, in which she explained why the Court's Fourth Amendment search and seizure doctrine has become "ill-suited [sic] to the digital age."[91] Sotomayor cautioned about the government's ability to monitor through GPS-enabled smartphones.[92] She expressed that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and recognized the consequential chilling effect.[93]

Underscoring how fast surveillance technology evolves and how slow Fourth Amendment jurisprudence responds to that change, Ferguson then discusses the advent of other big data surveillance technologies that the police currently use, including Automated License-Plate Tracker (ALPR) devices and facial-recognition cameras.[94] Facial-recognition technology with real-time video capabilities can enhance visual surveillance.[95] Facial recognition can also be assessed using the continuous feed from police-worn body cameras.[96] Another development is the Domain Awareness System (DAS) made by Microsoft for the NYPD.[97] DAS links 9,000 closed-circuit surveillance cameras in lower Manhattan feeding video to a digital alerts system tracking street movement, car license plates, and creating searchable images.[98] Aerial cameras like the Persistent Surveillance Systems offer real-time recordings of entire neighborhoods.[99] Moving beyond detailed descriptions of surveillance technology, Ferguson shows how data mining cell-tower numbers and metadata can assist criminal investigations. Data mining allows law enforcement to show, with a high probability, that "suspicious linkages" will connect a suspect to a

88. *See id.* at 416 (Sotomayor, J., concurring); *id.* at 419 (Alito, J., concurring).
89. *Id*. at 420 (Alito, J., concurring).
90. *Id*.; *see also* FERGUSON, *supra* note 7, at 100–101.
91. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); *see also* FERGUSON, *supra* note 7, at 100.
92. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).
93. *Id.*; *see also* FERGUSON, *supra* note 7, at 100.
94. FERGUSON, *supra* note 7, at 88–89.
95. *Id.* at 89
96. *Id.*
97. *Id*. at 86.
98. *Id*.
99. *Id*. at 89.

crime.[100] He offers the example of the FBI's using a simple digital search to track the High Country Bandits' connection to 16 small-town bank robberies over two years.[101] The FBI obtained a court order of all the cell phone tower records from four of the banks.[102] Because the cell phones regularly checked in with the nearest cell tower, the records offered a continuous log of cell phone numbers.[103] Consequently, the FBI correlated the location and the cell phone number to find the suspects.[104] Using that information, the FBI obtained a second court order seeking locational data from two cell phones. Through cell tower records, the FBI determined that one or both of the cell phones was near most of the 16 robberies.[105] Ferguson observes, "The probability that the High Country Bandit's cellphone coincidently would be at each of the banks at the exact time of the robberies is just too high to ignore. The probabilities suggest criminality and to a high degree of certainty."[106]

These kinds of investigations relying on cell phone records are commonplace.[107] In fact, the government's use of the third-party doctrine to subpoena records from wireless carriers dramatically accelerated as the sales of cell phones and smartphones increased exponentially in the last decade.[108] The two kinds of cell site location information (CSLI) central to data mining litigation are historical CSLI (indirect surveillance) referring to "records stored by the wireless service providers that detail the general location of a cell phone in the past," and prospective or real-time CSLI (direct surveillance), which is "all cell site information that is generated after the government has received court permission to acquire it."[109] Under the government's theory, the third-party doctrine allows agents to reach CSLI records or GPS data because: (1) phone service providers, not the phone users, own and maintain the records; (2) individuals do not expect privacy when they knowingly and voluntarily disclose their location information to the service provider; (3) people choose to have cell phones; and (4) CSLI shows only limited routing information.[110]

---

100. *Id*. at 124. Ferguson uses the term "suspicious linkages" to explain how cellular, digital, and biological data trails can be used to connect a suspect to a crime. *Id.*

101. *Id*. at 107.

102. *Id*. at 108.

103. *Id*. at 109.

104. *Id*. at 107.

105. *Id*.

106. *Id*. at 124.

107. *See id.* at 109. ("In the United States, police have used cell-tower searches in thousands of criminal cases.").

108. *See* Nick Sibilla, *Supreme Court's Cell Phone Tracking Case Could Hurt Privacy*, WIRED (Oct. 27, 2017), https://www.wired.com/story/supreme-courts-cell-phone-tracking-case-could-hurt-privacy/ (describing rise in smartphone ownership, CSLI gives law enforcement great power to track Americans through access to CSLI for criminal investigations).

109. *In re* Application U.S. for an Ord. Authorizing the Installation & Use of a Pen Reg. & a Caller Identification Sys. on Tel. Numbers (Sealed), 402 F. Supp. 2d 597, 599 (D. Md. 2005).

110. *See* FRIEDMAN, *supra* note 9, at 57.

Unfortunately, Ferguson did not have the benefit of discussing *Carpenter v. United States*[111] where the Court for the first time held that cell phone users possess a reasonable expectation of privacy in the CSLI history associated with their cell phones.[112] *Carpenter*'s inclusion could have reinforced Ferguson's analysis on pervasive surveillance. The majority concluded CSLI was not voluntarily exposed, and due to its revealing nature, was not subject to the third-party doctrine.[113] The facts were simple: Timothy Carpenter organized bands of robbers that held up nine Radio Shack and T-Mobile cell phone stores in Michigan and Ohio in 2010. Carpenter was apprehended after one of the suspects gave police the names and cell phone numbers of his 15 accomplices, including Carpenter.[114]

Relying on the Stored Communications Act, which requires a showing that the data was "relevant and material" to the ongoing investigation, prosecutors subpoenaed the records of Carpenter's general location information from his cell phone provider so they could connect his whereabouts over a four-month period with the dates, times, and locations of the robberies.[115] The government offered as evidence 186 pages of Carpenter's cell phone records from his wireless carriers MetroPCS and Sprint, placing Carpenter within a half-mile to two miles of the scenes of the robberies via the collection of 127 days of Carpenter's CLSI.[116] Carpenter unsuccessfully argued at trial that the government's collection of these records constituted a warrantless search in violation of the Fourth Amendment, and the cell tower information was key in convicting him.[117]

Chief Justice Roberts, writing for the majority, questioned the viability of the third-party doctrine in dicta. He observed that the vast amount of communicative information available today casually collected by wireless carriers, including CSLI, is exponentially greater than the slight personal information found in 1970s era bank records and landline phone records.[118] CSLI offers "a detailed and comprehensive record of the person's movements" which is more revealing than "several months of canceled checks, deposit slips and monthly statements" and records of "outgoing phone numbers."[119] Notably, *Carpenter* is a groundbreaking holding, but its scope is limited: it is not applicable to getting "tower dump" information about all of the phones that connected to a particular tower at a specific time, or "conventional surveillance techniques and tools, such as security cameras" or information collected for foreign affairs or national security.[120]

111. 138 S. Ct. 2206 (2018).
112. *Id*. at 2209, 2223–24.
113. *Id.*
114. *Id*. at 2212.
115. *Id*.
116. *Id*. at 2212, 2225.
117. *Id*. at 2212–13.
118. *Id*. at 2216–17.
119. *Id*.
120. *Id*. at 2220.

State courts are feeling the impact of *Carpenter*. In *State v. Muhammad*[121] the Washington Supreme Court held that the police tracking a cell phone ping is a search under the Fourth Amendment and the Washington state constitution requires a warrant absent exigent circumstances after finding that *Carpenter*'s reasoning applied to real-time CSLI by comparing historical CSLI to GPS monitoring.[122] In *Commonwealth v. Almonor*[123] the Massachusetts Supreme Court held that the police must get a warrant to track cell phones in historical or real time.[124] The court applied *Carpenter*'s analytical framework and reasoned that the intrusive nature of police action caused an individual's cell phone to transmit its real-time location, and raised distinct privacy concerns: "In today's digital age, the real-time location of an individual's cell phone is a proxy for the real-time location of the individual."[125]

C. Towards Big Data Policing Reform

Rise of Big Data Policing winds down with Ferguson proscriptively addressing some ways that big data helps police departments improve their training. Big data technologies can potentially improve police effectiveness, reduce police violence, and improve training and accountability through the application of surveillance technologies that law enforcement currently use on the public.[126] Such a systems-oriented approach to police practice will reveal recurring issues and offer opportunities for reform.[127] By turning the spotlight away from criminals and towards law enforcement, Ferguson shows how person-based predictive policing can recognize that certain individuals can be predicted to be more at risk for bad behavior, and this helps identify police officers who are more at risk for civilian conflicts and use of force.[128]

Looking forward, this proactive systems-based approach is focused on minimizing foreseeable risk, rather than punishing past conduct.[129] To illustrate, at one end systems can track officers who disproportionally or unlawfully use force and indicate when and where the incidents occur.[130] Data can also be uploaded to a database to track patterns of police contact in real time, creating a full crime map showing data about the interaction between crime and police. Ferguson says this live monitoring improves police efficiency while strengthening community accountability.[131] At the other end, real-time tracking allows police administrators to monitor individual officers to evaluate

121. 194 Wash.2d 577 (2019).
122. *Id*. at 580.
123. 120 N.E.3d 1183 (2019).
124. *Id*. at 1187.
125. *Id*. at 1194.
126. FERGUSON, *supra* note 7, at 143.
127. *Id*. at 162.
128. *Id*. at 147.
129. *Id* at 148.
130. *Id*. at 144.
131. *Id*. at 145.

performance.[132] In addition, mapping police patrols over time can provide insight about the efficacy of patrol design.[133] Further, the mining of police data reveals efficiencies, bias, and avenues to improve accuracy and fairness in routine policing methods.[134]

II. BIG DATA POLICE INVESTIGATIONS, COST-BENEFIT THEORY, MOSAIC SEARCHES, AND THE THIRD-PARTY DOCTRINE

Smart Surveillance offers an alternative framework of understanding how emerging security technology and privacy can coexist, and it serves as a rejoinder to those who view big data surveillance, in any form, as a threat to privacy rights.

A. Arguing for More Big Data Police Investigations and Mosaic Searches

At the outset, Simmons suggests big data is revolutionizing criminal investigation and has the potential to dramatically increase the productivity of surveillance.[135] Big data analysis provides police and judges with tools that predict future behavior with greater precision than ever before. Big data is derived from the collection of immense amounts of information from different sources and processes using statistical analysis to create results called "mechanical predictions."[136] Big data tools increase fairness when they are objectively applied to critical decision points in investigations and prosecutions.[137] Mechanical predictions can be used to assist decision makers in deciding how to more effectively allocate police resources, notify police of potentially dangerous individuals at specific locations, identify criminal actors and criminal activity from social media posts, advise judges making pretrial detentions decisions, and provide guidance to judges at sentencing.[138] Additionally, mechanical predictions are not considered a "search" under the Fourth Amendment because the data gathering is from public sources, and thus there is no need to establish reasonable suspicion or probable cause. [139]

Embracing the great advantages presented by big data, Simmons proposes a new cost-benefit approach to the Fourth Amendment that accommodates new surveillance technologies and strong privacy protections in the form of an ambitious plan for using data-driven policing technologies towards quantitative justice grounded in data theory and law.[140] Relying on abstract case studies, algorithms, data sets, equations, methodologies, statistical studies, and opinion

132. *Id*. at 146.
133. *Id*.
134. *Id*. at 150.
135. *See* SIMMONS, *supra* note 8, at 67.
136. *Id.* at 37.
137. *Id.* at 67.
138. *Id.* at 37.
139. *Id.* at 38.
140. *Id.* at 2.

surveys, Simmons offers his thesis: modern surveillance techniques need methods of evaluation and regulation based on a new paradigm measuring the efficiency of the new technology in comparison with the efficiency of existing surveillance techniques.[141]

Undoubtedly, Simmons supports the government's need for effective investigatory surveillance methods much more than Ferguson. Big data's predictive algorithms represent an opportunity to increase the accuracy and transparency of surveillance.[142] Simmons wants widespread adoption of predictive algorithms which will result in greater precision determining benefits of a particular surveillance.[143] Interestingly, Simmons's new conceptualization of the Fourth Amendment requires maintaining the government's ability to use "mosaic searches"—a detailed and aggregated account of a person's movements and/or individual pieces of information collected from surveillance that reveals more than the sum of the parts.[144]

Simmons considers the benefits of mosaic searches as an inexpensive tool for investigating criminal activity.[145] Law enforcement deployment of low-cost surveillance methods such as public surveillance cameras, body cameras, drones, and robots will provide police with massive amounts of video and information that can be used for mosaic searches and to create comprehensive permanent records.[146] But there is pushback by some Fourth Amendment scholars like David Gray, who is wary of big data's privacy-eroding potential, and is critical of the mosaic theory. He professes, "The mosaic theory can guarantee only that governmental agents are not gathering too much information about us. This is cold comfort indeed if it remains the case that the government may well be tracking, and surveilling any of us or all of us at any particular moment."[147] He posits the police take advantage of the absence of constitutional protection for public activities seen in ordinary surveillance.[148] More to the point, Gray argues the mosaic theory presents a line-drawing problem where officers cannot determine whether a search requires a warrant in an active investigation gathering information from human surveillance, public records, searches, meta data, and witness interviews.[149]

Nevertheless, Simmons argues against the efforts made by the Court to limit mosaic searches. He contends mosaic searches have been weakened by the *Jones* and *Carpenter* rulings that have specifically created legal barriers to continuous public surveillance.[150] According to Simmons, the *Jones* concurrence's

141. *Id.*
142. *Id.* at 63.
143. *Id*.
144. *Id.* at 120.
145. *Id.* at 121.
146. *Id.* at 133, 187.
147. *See* GRAY, *supra* note 9, at 115.
148. *Id.* at 98
149. *Id*.
150. SIMMONS, *supra* note 8, at 125.

reasoning completely ignores any cost-benefit analysis.[151] Simmons perceives the *Jones* opinion as successfully identifying the privacy costs associated with mosaic searches, but failing to account for the increased benefits.[152] In analyzing *Carpenter*, Simmons relays that the Court overreacted in finding a warrant requirement for access to all public data collection and mosaic searches.[153] In particular, he takes issue with *Carpente*r's reasoning and disagrees with the invocation of social theory by the majority to argue that there is a distinctive, more intimate privacy cost to these searches, because law enforcement officers gather information from massive amounts of public data.[154] According to Simmons, the Court missed an opportunity to highlight the benefits of low-cost, less labor-intensive public surveillance that leverages law enforcement resources and increases security in an efficient manner.[155] To him, mosaic searches based on public information reveal little personal information and the privacy costs are low.[156]

In Simmons's world, mosaic searches offer another benefit: public surveillance will treat everyone the same, regardless of socio-economic class.[157] The lower financial costs for tracking GPS devices and public surveillance cameras will canvass lower-income neighborhoods, as well as affluent neighborhoods, at the same heightened level of police surveillance.[158] This serves as a "redistribution" or "near equalization" of privacy.[159] Simmons adds, "[W]e could reduce the privacy cost of these low-cost collection techniques by combining them with algorithms that analyze patterns of behavior and detect those patterns that indicate a high likelihood of criminal behavior."[160]

As an alternative, Simmons suggests the Court replaces its practice of striking a balance between police power and civil liberties in Fourth Amendment cases dealing with new technology with a cost-benefit analysis.[161] Within this matrix, administrative costs and privacy costs that weigh against the benefits of surveillance of potential criminal activity, and the amount of resources/administrative costs used in conducting the surveillance, are weighed against the degree of its privacy infringement.[162] The author asserts that applying economic principles to Fourth Amendment law allows the criminal justice system to maximize output and minimize costs, while respecting the constitutional rights of citizens.[163] Also, a cost-benefit analysis harmonizes the

151. *See id.* at 126.
152. *Id*.
153. *Id.* at 166.
154. *Id.* at 125–126.
155. *Id.* at 127.
156. *Id.* at 130.
157. *Id.* at 135.
158. *Id.* at 137
159. *Id.*
160. *Id.* at 187.
161. *Id.* at 5.
162. *Id.* at 5, 10, 18.
163. *Id.* at 14.

decision-making process for the police by allowing the police to determine the pros and cons of spending money on training or buying new surveillance tools, and assess the effectiveness of these choices.[164]

Cost-benefit analysis allows courts to adjust the legal standard of suspicion that law enforcement must show before using different surveillance methods. Under this schema, law enforcement retains discretion in deciding when to act before obtaining legal authority and the productivity value can be used to gauge whether or not to use a particular type of surveillance.[165] For productive searches with a high likelihood of obtaining evidence of criminal activity, the police can run searches without first getting a warrant if the requisite level of suspicion is achieved, and law enforcement can prove that the search is the least restrictive means of obtaining the information in less productive searches.[166]

Against this backdrop, Simmons prescribes his remedy: (1) the Court needs to realign its "reasonable expectations of privacy" analysis post-*Katz v. United States*;[167] (2) the new legal standard must incorporate new quantitative tools like big data algorithms that predict criminal behavior; and (3) the Court must expand the number of legal standards applicable to surveillance so that each standard matches the level of intrusiveness.[168]

*Smart Surveillance'*s theme of strongly critiquing the Court's Fourth Amendment technology surveillance decisions and preserving the government's ability to effectively conduct investigations strikes a high note in a chapter entitled "The Third-Party Doctrine Dilemma and the Outsourcing of Our Fourth Amendment Rights."[169] Here, Simmons argues that transactional surveillance should not be subject to Fourth Amendment oversight.[170] For the uninitiated, "the third-party doctrine may be the most critiqued aspect of Fourth Amendment jurisprudence"[171] since being established forty-something years ago by the leading cases: *United States v. Miller*[172] and *Smith v. Maryland*.[173] Simmons considers the third-party doctrine as "anachronistic" given that today's technology society casually shares information with third-parties in the form of emails, internet searches history, and cloud storage, yet he wants to preserve it.[174] Even as a guardian of the third-party doctrine, he says it is unreasonable to think

164. *Id.* at 15.
165. *Id.* at 35.
166. *Id.* at 16.
167. *See* Katz v. United States, 389 U.S. 347 (1967) (petitioner relied on the privacy of a phone booth when making illegal gambling wagers not knowing that federal agents had covertly attached an electronic listening and recording device onto the outside).
168. *See* SIMMONS, *supra* note 8, at 4–5 (2019).
169. *See generally id.* at 141–62.
170. *Id.* at 153–54.
171. *Id.* at 146.
172. 425 U.S. 435 (1976) (holding that respondent had no reasonable expectation of privacy in information voluntarily conveyed to bank).
173. 442 U.S. 735 (1979) (holding that petitioner had no reasonable expectation of privacy in information voluntarily conveyed to the telephone company).
174. *See* SIMMONS, *supra* note 8, at 144, 146 (2019).

that a person "assumes the risk" that the government can get emails, internet searches, and car location.[175]

Although *Carpenter* retreated from the third-party doctrine, Simmons believes it still serves a critical function and will always exist in Fourth Amendment jurisprudence.[176] In this chapter, Simmons shows his fondness for the third-party doctrine which allows police to get information from informants and others who want to help the police.[177] Absent the third-party doctrine, Simmons says, criminals will conceal their illegal activities, maintain secrecy over their interactions with undercover agents, and store incriminating information with third-party companies.[178]

Simmons applies the cost-benefit analysis to the situation when the police want to get information without a warrant and suggests that security benefits and efficiencies of allowing access to the information are weighed against the privacy costs of revealing the information.[179] The privacy cost is empirically determined by the third-party doctrine's underlying rationale: "people abandon their expectation of privacy when they share information with third parties."[180] Accordingly, Simmons urges courts to allow third parties to determine the degree in which they want to protect their customer's information, thereby preserving autonomy of the third parties, and allow them to set their own standards regarding when they want to report crimes and when they want to fight to protect their customer's privacy.[181] In turn, consumers can examine these standards and then choose which companies they want to trust with their information.[182]

Simmons suggests that too much attention has been focused on the rights of the defendant, and he favors enhancing and enforcing the Fourth Amendment rights of the third parties themselves, so that they can object to information requests on their own behalf.[183]

Perhaps Simmons can find solace in Kennedy's dissent in *Carpenter* where he deemed the third-party doctrine is as viable as ever. Kennedy strenuously argued that the third-party doctrine controls CSLI business records, and therefore the government has a legal right to obtain them without a warrant.[184] He criticized the majority for using a category-by-category balancing test instead of strictly applying *Miller* and *Smith*:

---

175. *Id.* at 144.
176. *Id.* at 146.
177. *Id.* at 147.
178. *Id.* at 147, 161; *see also* Christopher Slobogin, *Policing, Databases, and Surveillance*, 18 CRIMINOLOGY, CRIM. JUST., L. & SOC'Y 70, 72 (2017) (using the example of cloud-based searches by the government and discussing how a probable cause requirement may "handcuff legitimate government efforts to nab terrorists and criminals").
179. *See* SIMMONS, *supra* note 8, at 154, 161.
180. *See id.* at 154.
181. *Id.*
182. *Id.* at 161.
183. *Id*. at 141.
184. *Carpenter*, 138 S. Ct. at 2223–24 (Kennedy, J., dissenting).

> "The majority opinion misreads this Court's precedents, old and recent, and transforms *Mille*r and *Smith* into an unprincipled and unworkable doctrine. The Court's newly conceived constitutional standard will cause confusion; will undermine traditional and important law enforcement practices; and will allow the cell phone to become a protected medium that dangerous persons will use to commit serious crimes."[185]

To the dismay of third-party critics, Kennedy made no distinction at all between cell site records and financial/telephone/business records. To him, cell phone customers like Carpenter simply have no possessory interest in them because CSLI is controlled and owned by the cell phone service provider, not by its customer.[186] He argued the government has always had a longstanding lawful practice in collecting credit card information and records for vehicle registration, hotel stays, employment, and utility bills—regardless of their personal and sensitive nature.[187] According to Kennedy, the *Smith*/*Miller* voluntariness requirement is also satisfied, since Americans are aware that they have a lesser expectation of privacy in the digital age and voluntarily share their location with the public via social media.[188]

But Kennedy's and Simmons's enthrallment over the third-party doctrine is countered by Justice Gorsuch's *Carpenter* dissent, outlining the shortcomings of the third-party doctrine.[189] Gorsuch explains how *Smith/Miller* were unfortunate byproducts of *Katz*. He considers *Smith/Miller* as "a doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."[190] Gorsuch observed: (1) "The facts that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them,"[191] and (2) "[J]ust because you *have* to entrust a third-party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it."[192]

The third-party doctrine has also fallen out of favor with many lower courts. For instance, even before *Carpenter*, the Fourth and Eleventh Circuits were already declining to apply the third-party doctrine in surveillance cases.[193] With

185. *Id.* at 2230. (Kennedy, J., dissenting).

186. *Id.* at 2224. (Kennedy, J., dissenting).

187. *Id.* at 2233, 2228–29. (Kennedy, J., dissenting).

188. *Id.* at 2232. (Kennedy, J., dissenting).

189. *Id.* at 2262. (Gorsuch, J., dissenting) (describing the general difficulties of applying *Smith* and *Miller* in the modern digital era and risking a reduction of Fourth Amendment protections).

190. *Id.* at 2264. (Gorsuch, J., dissenting).

191. *Id.* at 2267. (Gorsuch, J., dissenting).

192. *Id.* at 2271. (Gorsuch, J., dissenting). Gorsuch looks to positive law for guidance on evolving technologies and proposes a property rights-based argument. Under Gorsuch's property rights-based theory of the Fourth Amendment, Carpenter had a property interest in his cell phone data. *Id.*

193. An en banc Fourth Circuit in *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015) (en banc), abrogated by *Carpenter*, 138 S. Ct. at 2206, found the third-party doctrine inapplicable to the facts and held that the government's warrantless procurement of CSLI for 221 days in an

the blessing of *Carpenter*'s rationale, future courts should feel reasonably confident to conclude that the third-party doctrine is inapplicable and to follow the majority of federal courts considering the issue of whether there is a reasonable expectation of privacy in real-time CSLI. These courts concluded CSLI information may only be obtained pursuant to a warrant supported by probable cause because it effectively converts the cell phone into a tracking device.[194]

B. Hyper-Intrusive Searches and the Fourth Amendment

In the last chapter, Simmons investigates "hyper-intrusive searches": electronic eavesdropping devices and hidden cameras installed in homes or offices to monitor long-distance people in private places, microphones that can listen through windows, and radar devices.[195] He explains these devices provide low and broad levels of useful information compared to the privacy costs imposed.[196] As such, whenever the government uses hyper-intrusive surveillance methods, courts need to require higher standards of certainty before imposing specific requirements like minimization, least intrusive tests, time limitations, or limiting the surveillance to serious crimes.[197] Simmons says this would increase the productivity of the search by lowering the privacy costs of potential intrusive searches.[198] Also, law enforcement officials should be required to empirically demonstrate that the benefits outweigh those offered by

investigation of robberies violated the Fourth Amendment. Yet the court allowed the government to use the CSLI under the "good faith" exception to the exclusionary rule. *Graham*, 796 F.3d at 362. A complementary view was conveyed by Judge Martin's insightful dissent challenging the reach of the third-party doctrine in *United States v. Davis*, 785 F.3d 498, 533 (11th Cir. 2015) (en banc) (Martin, J., dissenting), abrogated by *Carpenter*, 138 S. Ct. at 2206. Martin disagreed with an *en banc* Eleventh Circuit's holding that there was no search in the collection of a third-party telephone company's business records, and that historical cell tower location information for a 67-day period did not violate the Fourth Amendment under the SCA. *Id.* at 512.

194. *See, e.g.*, United States v. Espudo, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013) (reasonable expectation of privacy in prospective cell phone location information, concluding real-time cell phone data not business records under the Stored Communications Act); *see also In re* U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 849 F. Supp. 2d 526, 539–42 (D. Md. 2011) (reasonable expectation of privacy in location and movements revealed by cell phone data); *see also In re* U.S. for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone No. ESN, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006) (same: probable cause required for cell phone tracking data warrant); *see also In re* U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (same); *see also In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (expressly limiting its holding to historical data).

195. *See* SIMMONS, *supra* note 8, at 162–63.

196. *Id.* at 164.

197. *Id.* at 182

198. *Id.*

less intrusive surveillance methods.[199] After a determination of the costs and benefits, courts may then permit the government to engage in these searches.[200]

The Court addressed one example of hyper-intrusive searches in *Riley v. California*,[201] one of the most important substantive Fourth Amendment cases. In *Riley*, the Court addressed whether an officer's search of a defendant's smart phone incident to an arrest violated the Fourth Amendment, and ruled unanimously that police generally must obtain a warrant to search the contents of cell phones.[202] Chief Justice Roberts, writing for the majority, recognized that today's cell phones, which are used pervasively, are essentially powerful minicomputers that function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers" and recognized the privacy interests implicated in data stored in modern cell phones showing internet searches, browsing history, and other personal information.[203] Foreshadowing *Carpenter*, the Court reasoned the third-party doctrine did not apply because: (1) the defendant did not voluntarily consent to and was unaware of the cell phone company's collection of his or her location information; and (2) cell phone data is "qualitatively different" from ordinary physical records as it reveals much more personal information than older technologies.[204]

C. Terry v. Ohio *and Marijuana Traffic Stops*

Like Ferguson, Simmons also questions *Terry*'s broad allowance of frisks of suspects during a stop if the officer has "reason to believe" the suspect is armed.[205] Here, Simmons critiques *Terry* and the manner in which courts crafted broad standards to accommodate the subjective judgments and beliefs of officers on the street.[206] Simmons cautions that this is not the most accurate assessment and prefers judges be required to qualify the likelihood that the frisk would reveal a weapon, and then make a more objective evaluation of whether the reasonable suspicion legal standard has been met.[207]

In a world of predictive algorithms, Simmons says the police officer seeking a search warrant would present the judge with the outputs of a computer program showing a high probability that contraband will be found.[208] A predictive algorithm would reduce the reliance on proxies for race, such as observing a person in a "high crime" area which tend to be inner city communities of color, and is associated with the unconscious racial biases of

199. *Id.*
200. *Id.*
201. 573 U.S. 373 (2014).
202. *Id.* at 401.
203. *Id.* at 393–94.
204. *Id.* at 395–96.
205. *See* SIMMONS, *supra* note 8, at 42.
206. *Id.* at 66–67.
207. *Id.* at 42.
208. *See id.* at 72.

police officers and judges, in determining reasonable suspicion or probable cause.[209] Simmons builds on Ferguson's analysis and uses *Terry* to apply quantified factors to illustrate the usefulness of the predictive algorithm and the outcome determinative model.[210] Simmons says if the facts of *Terry* were replayed in the modern era, McFadden would use facial recognition technology to identify Terry and learn of his prior criminal record through a database search, connect Terry through license data to other unsolved robberies in the area, and apply McFadden's observations of Terry pacing, looking, and conferring.[211]

Astute readers will begin to realize here that Simmons's discussions about race and surveillance are noticeably less comprehensive than those offered by Ferguson. Nonetheless, Simmons's ideas are worthwhile. First, Simmons approves of properly designed algorithms that explicitly use race if "there would be empirical statistical proof that in the given context, race did help determine whether or not an individual was guilty of a crime."[212] Second, Simmons maintains that mechanical predictive algorithms are more effective than the current system that counts on implicit biases held by police officer and judges.[213] Third, Simmons concedes that not all residue of racial discrimination can be removed from existing databases, and police officers and judges will continue to make mistakes using the predictive algorithms as the baseline and adding their independent observations.[214]

A point of contention I had with *Smart Surveillance* was its minimal attention to traffic stops. While Simmons mentions in passing that the Court has inconsistently applied the Fourth Amendment in stopping and searching cars without warrant, [215] this issue deserves more attention in a book about the Fourth Amendment. Traffic stops are the most common interaction society has with law enforcement, yet many United States residents are unaware of the many tactics officers employ to pull over cars hoping to find contraband.[216] Police also exercise broad authority to routinely pull over cars for almost any alleged traffic

209. *Id.* at 50.

210. *Id.* at 58–59.

211. *Id.*

212. *Id.* at 48. When Simmons refers to various contexts wherein law enforcement explicitly refer to the race of a person, he provides the examples of an officer looking for immigrants at the Mexico border and a person who seems out of place because of their race, such as a white person in a predominantly black neighborhood. *Id*.

213. *Id.* at 63.

214. *Id.*

215. *Id.* at 3.

216. *See* David Moran, *The New Fourth Amendment Vehicle Doctrine: Stop and Search Any Car at Any Time*, 47 VILLANOVA L. REV. 815, 819 (2002) (arguing that motorists should be aware that a police officer can lawfully stop and search cars for any almost reason and at any time); *see also* David A. Sklansky, *Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment*, 1997 SUP. CT. REV. 273, 273 (1997) (explaining that police officers "can eventually pull over almost anyone they choose").

violation, including having tinted windows, having a broken taillight, crossing over a fog line, or some other inventive pretext.[217]

"The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained."[218] The Court has long held that "[i]f a car is readily mobile and probable cause exists to believe it contains contraband, the Fourth Amendment . . . permits police to search the vehicle without more."[219] This exception to the warrant requirement is often referred to as the "automobile exception."[220] Probable cause, for purposes of the automobile exception, must be "based on objective facts that could justify the issuance of a warrant."[221] The Court has upheld, in a long line of cases, the notion that probable cause exists when "there is a fair probability [that] contraband or evidence of a crime will be found in a particular place."[222]

James Foreman Jr. refers to pretextual traffic stops as an easy tool for police to stop drivers as they please, stating, "if a car draws suspicion from the police, they can almost invariably find a way to stop it legally, especially if they follow it long enough"[223] and follow up with an explanation of one of the "techniques" the police use to secure consent.[224] This is commonly seen in cases where an officer says he smelled the odor of marijuana as justification for searching a car during a traffic stop.[225] However, it is problematic to rely on odor alone given the amount of time the odor has been present, the mobility of the odor, and the inability to immediately attribute an odor to an identifiable source.[226] Thus, in

217. *See, e.g.*, Elizabeth E. Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CAL. L. REV. 199, 210 (2007) (reporting that "arrests for drugs and firearms charges are often the result of stops ostensibly for broken taillights, driving too slowly, or too quickly, or failing to signal, is well-documented"); Harvey Gee, *"U Can't Touch This" Fog Line: The Improper Use of a Fog Line Violation as a Pretext for Initiating an Unlawful Fourth Amendment Search and Seizure*, 36 N. ILL. UNIV. L. REV. 1, 2 (2015) (describing how police are initiating traffic stops based on allegations that drivers crossed onto a fog line in violation of state ordinance); Melanie D. Wilson, *"You Crossed the Fog Line!"—Kansas, Pretext, and the Fourth Amendment*, 58 U. KAN. L. REV. 1179, 1191 (2010) (same).

218. California v. Acevedo, 500 U.S. 565, 580 (1991).

219. Pennsylvania v. Labron, 518 U.S. 938, 940 (1996).

220. United States v. Ross, 456 U.S. 798, 808 (1982).

221. *Id.*

222. United States v. Grubbs, 547 U.S. 90, 95 (2006).

223. JAMES FOREMAN, JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 198 (2017); *see also* Tracy Maclin, Cops and Cars: How the Automobile Drove Fourth Amendment Law, 99 BOSTON U. L. REVIEW 2317, 2346–47 (2019) (explaining how and why traffic stops by police are often a ruse to go on "fishing expeditions for criminal conduct.").

224. FOREMAN, JR., *supra* note 223, at 200.

225. *See* Ned Oliver, *When Police Say They Smell Pot, They Can Search You. Lawmakers Worry Decriminalization Won't Change That*, VIRGINIA MERCURY, Jan. 24, 2020, https://www.virginiamercury.com/2020/01/24/when-police-say-they-smell-pot-they-can-search-you-lawmakers-worry-decriminalization-wont-change-that/.

226. Michael A. Sprow, *Wake Up and Smell the Contraband: Why Courts that do not Find Probable Cause Based on Odor Alone Are Wrong*, 42 WM. & MARY L. REV. 289, 302 (2000).

court it is difficult to prove what an officer did or did not smell.[227] The odor of marijuana alone as a reason to conduct a warrantless search is especially problematic during the age of marijuana decriminalization and legalization.[228] Since 2012, eleven states and Washington, D.C., have legalized small amounts of marijuana for recreational purposes.[229] Fifteen more states have decriminalized marijuana; possession of small amounts of marijuana no longer carries jail or prison time.[230] Thirty-six states and Washington, D.C., permit the use of medical marijuana within state-specific regulations.[231]

Consider this hypothetical showing the ease in which officers can falsely claim that they smelled the odor of marijuana justification as a ruse to search a car to more easily develop the probable cause needed to make an arrest. Let's say Officer Smith testifies at a motions hearing that he noticed the defendant's expired registration tags, initiated a traffic stop, and as he approached the car, he noticed the strong smell of burnt marijuana. The rule is if during a routine traffic stop an officer sees, smells, or learns of evidence of another crime they can shift the detention to investigate this other illegal activity.[232] Smith based the detention on a suspected violation of unlawfully possessing an open container or open package of cannabis or cannabis products while driving. The focus of the traffic stop then shifts to an investigation of the marijuana. Although the defendant did not consent to Smith's request to search, the officer searched anyway. While no marijuana was found, the officer did come across two zip lock bags containing crack cocaine inside a compartment under the passenger seat and a gun inside a compartment under the driver's seat.

227. *See* Michael Rubinkam, *In Era of Legal Pot, Can Police Search Cars Based on Odor?*, U.S. NEWS & WORLD REP., Sept. 13, 2019, https://www.usnews.com/news/us/articles/2019-09-13/in-era-of-legal-pot-can-police-search-cars-based-on-odor.

228. *See id*; Oliver, *supra* note 225.

229. *See* German Lopez, *Marijuana Has Been Legalized in 11 States and Washington*, VOX, June 25, 2019, https://www.vox.com/identities/2018/8/20/17938336/marijuana-legalization-states-map.

230. *See id*.

231. *See* Legal Medical Marijuana States and DC, ProCon.org., Dec.3, 2020, https://medicalmarijuana.procon.org/legal-medical-marijuana-states-and-dc/.

232. During the course of this shift, ordering defendant out of the car is a non-issue. Even for a routine traffic stop (e.g., a registration violation as here) a driver can be ordered out of the car with no additional justification needed. *See* Arizona v. Johnson, 555 U.S. 323, 331 (2009) (discussing Pennsylvania v. Mimms, 434 U.S. 106 (1977)). Additionally, California Health & Safety Code § 11362.3(a)(7) does not permit any person to "Smoke or ingest cannabis or cannabis products while driving, operating a motor vehicle, boat, vessel, aircraft, or other vehicle used for transportation." As stated in *People v. Russell*, "facts which come to light during detention may provide reasonable suspicion to prolong detention." 81 Cal. App. 4th 96, 102 (Cal. Ct. App. 2000). If additional cause to detain develops after the initial stop, additional time to investigate is allowed. *Id.*; *see also* People v. Espino, 247 Cal. App. 4th 746, 756 (Cal. Ct. App. 2000) ("If the police develop reasonable suspicion of some other criminal activity during a traffic stop of lawful duration, they may expand the scope of the detention to investigate that activity.").

Was it unreasonable for Smith to shift the traffic stop to investigate? Was the initial detention prolonged?[233] Arguably, the prolongation began when the officer asked if there was "anything illegal in the car." This question has nothing to do with the expired tags detention. Within the meaning of the Fourth Amendment, an individual is detained when police officers restrain their liberty by means of physical force or show of authority.[234] The test for whether a police officer's conduct amounts to a detention is whether the officer's conduct would indicate to a reasonable person that they are not free to leave or to otherwise terminate the encounter.[235] In determining whether a reasonable person would have believed they were free to leave or end the encounter, a court must take into account the totality of the circumstances from the perspective of a reasonable person in the defendant's position.[236]

The issue at the motions hearing will be: did Officer Smith have probable cause to believe the defendant had marijuana in their car because he smelled marijuana? The answer depends on whether Smith truthfully smelled burnt marijuana or fabricated his account to justify the search of the car. The prosecutor could argue that the officer's account is credible and will rely on legal authority that supports such a position. They could rely on *People v. Fews*,[237]

233. *See* People v. McGaughran, 25 Cal. 3d 577, 579 (Cal. 1979) (holding that a traffic stop that is lawful at its inception may "exceed constitutional bounds when extended beyond what is reasonably necessary under the circumstances which made its initiation permissible."); *see also* People v. Medina, 110 Cal. App. 4th 171, 176 (Cal. Ct. App. 2003) (same). The United States Supreme Court has articulated the same rule. *See* Illinois v. Caballes, 543 U.S. 405, 407 (2005) ("A seizure that is justified solely by the interest in issuing a warning ticket to the driver can become unlawful if it is prolonged beyond the time reasonably required to complete that mission.").

234. Sometimes a defendant does not feel free to end an interaction with the police. *See e.g. In* re Manuel G., 16 Cal.4th 805, 821 (Cal. 1997) (detention does not occur when officer merely approaches an individual on the street and asks a few questions; seizure occurs only when officer restrains the individual's liberty by means of physical force or show of authority); People v. Linn, 241 Cal. App. 4th 46, 50; 53–54; 64 (Cal. Ct. App. 2015); United States v. Mendenhall, 446 U.S. 544, 554 (1980) (holding that an objectively reasonable person would not have felt free to terminate an encounter based on authoritative commands made by an officer who made pointed statements about the conduct of the passenger of a car; commanded the passenger to put out her cigarette and put down her soda can; questioned the passenger for personal details while recording the information on a form; told the driver to stop after she tried to walk away; and told the defendant to stand next to him as he checked her eyes and investigated sobriety); People v. Garry, 156 Cal. App. 4th 1100, 1104, 1112 (Cal. Ct. App. 2007) (finding a detention when the officer bathed a spotlight on the defendant who was standing on a street. The officer then got out of his car, and quickly walked up to him while simultaneously asking him about his probation/parole status); People v. Kidd, 36 Cal. App. 5th 12, 15, 22 (Cal. Ct. App. 2019) (concluding that no reasonable person in the defendant's position would have felt free to leave when a police officer made a U-turn and parked 10 feet behind the defendant's parked car, which had another car parked 10 feet in front of it, and he trained the driver-side mirror spotlight and the overhead bar light in tandem onto the defendant).

235. *Mendenhall*, 446 U.S. at 554.

236. People v. Parrott, 10 Cal. App. 5th 485, 493 (Cal. Ct. App. 2017) ("In determining whether a reasonable person would have believed he or she was free to leave the encounter, a court must take into account the totality of the circumstances from the perspective of a reasonable person in the defendant's position.").

237. 27 Cal. App. 5th 553 (Cal. Ct. App. 2018).

where the officer believed that the defendant was involved in criminal activity because the officer saw a rerolled cigar and smelled marijuana, and there was evidence suggesting that contraband would be found in the vehicle. The court determined that the odor and presence of marijuana, as well as the continuous and furtive movements by Fews inside the SUV, were sufficiently unusual to raise the officer's suspicions that the men were involved in criminal activity related to drugs and could be armed.[238]

Conversely, the defense counsel may argue that the testimony from Smith was not credible and urge the court to apply *contra* authority. They could cite to a case such as *People v. Lee*,[239] where the sole motivation of San Diego Police Department officers was to investigate for probable criminal behavior and look for incriminating evidence.[240] The court held the officer lacked probable cause to believe evidence of illegal activity would be found in the vehicle.[241] The court concluded that even considering the totality of circumstances known to the officer, there did not exist a fair probability that contraband or evidence of a crime would be found and therefore the court affirmed the order granting Lee's motion to suppress.[242]

Oftentimes, judges find the police to be credible and find that probable cause existed based on the police officer's testimony that the defendant had marijuana in their car because the officer smelled the odor of burnt marijuana. The large spike of cases involving officer reliance on the odor of marijuana as justification for a search has led at least one New York judge to strongly question the credibility of officers claiming they smelled marijuana.[243] Judge April Newbauer called on New York judges to stop being so deferential to officer claims of smelling marijuana, saying, "the time has come to reject the canard of marijuana emanating from nearly every vehicle subject to a traffic stop."[244]

In the final analysis, Simmons's ambitious plan to resolve the tensions between police surveillance and the government's interest in policing versus an individual's right to privacy has initial appeal. But as discussed in Section II, it cannot withstand the realities of modern policing, which all too often run roughshod over the Fourth Amendment, nor a Court that has brought reasonable expectation of privacy into the digital age with its recent surveillance technology rulings.

---

238. *Id*. at 561.

239. 40 Cal. App. 5th 853 (Cal. Ct. App. 2019).

240. *Id*. at 869.

241. *Id*. at 866–67.

242. *Id*. at 869–70.

243. *See* Joseph Goldstein, *Officers Said They Smelled Pot. The Judge Called Them Liars*, N.Y. TIMES, Sept. 13, 2019, https://www.nytimes.com/2019/09/12/nyregion/police-searches-smelling-marijuana.html; *see also* Alice Speri, *A New York Police Officer Was Caught on Camera Apparently Planting Marijuana in a Car—For the Second Time*, THE INTERCEPT, Mar. 18, 2020. https://theintercept.com/2020/03/18/nypd-misconduct-body-cameras-marijuana (acknowledging a Bronx judge questioning the credibility of officer testimony about smelling marijuana).

244. *See* Goldstein, *supra* note 243.

III. RECENT FOURTH AMENDMENT DEVELOPMENTS: POLE CAMERA SURVEILLANCE, STINGRAY CELL-SITE SIMULATORS, AND FACIAL RECOGNITION AND FACIAL SURVEILLANCE TECHNOLOGY

This last section examines recent developments in surveillance technology and Fourth Amendment jurisprudence and focuses on some of the most popular and powerful surveillance tools used by local police departments with little oversight: pole cameras, Stingray cell-site simulators, and facial recognition and facial surveillance technology. As with their predecessors, these newer technologies purportedly help police fight crime, but they can also infringe on privacy rights.

A. Pole Camera Surveillance and the Fourth Amendment

Given the comprehensive scope of *Rise of Big Data Policing* and *Smart Surveillance*, I was surprised that the authors missed the opportunity to discuss more routine surveillance tools like 24/7 video surveillance pole cameras placed outside of the home. Pole cameras are video cameras mounted by the police on utility poles or other fixed locations that continuously record everything that happens on a suspect's property, often for months at a time.[245] Police can control the camera remotely using pan, tilt, and zoom features and can review past footage at any time to look for activity patterns and visitors.[246]

While the cameras have increased in sophistication, their use for surveillance purposes has been a longstanding point of contention between law enforcement and privacy advocates, like Christopher Slobogin, who are especially weary of camera surveillance mounted on buildings and on telephone poles. Slobogin argues the Fourth Amendment should apply limitations on how government agencies use closed circuit CCTV as public surveillance cameras.[247] Slobogin finds the Court's roadblock decisions such as *City of Indianapolis v. Edmond*[248] to be instructive and thinks that public cameras should be authorized only when roadblocks would be authorized.[249] The *Edmond* Court ruled that police roadblocks aimed at discovering drugs violated the Fourth Amendment's prohibition against searches and seizures that are based on reasonable suspicion.[250] Justice O'Connor, writing for the Court, stated that law enforcement roadblocks must have a specific purpose outside the normal purpose of preventing crime generally.[251] The state must have a strong interest in that purpose, the roadblock must be an effective way to achieve that purpose, and the roadblock cannot excessively intrude on the privacy of innocent individuals

245. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 214, 216 (2002).
246. *Id.* at 220.
247. *Id.* at 217.
248. 531 U.S. 32 (2000).
249. Slobogin, *supra* note 245, at 295.
250. *Edmond*, 531 U.S. at 48.
251. *Id.* at 44.

stopped in the roadblock.[252] Applying the *Edmond* rationale to CCTV, Slobogin argues that the "primary purpose" of CCTV is to implement the government's general interest in crime control.[253] Under this theory, *Edmond* could be interpreted to prohibit government use of cameras and, absent extraordinary circumstances, *Edmond* suggests cameras intensively focused on an individual should be allowed only when there is individualized suspicion.[254]

For decades, many courts have concluded CCTV surveillance does not violate the Fourth Amendment, analogizing it to ordinary surveillance by a police officer in a public space or utility worker sitting atop the pole observing the same activities the camera recorded.[255] However, some recent court rulings illustrate how the government's video surveillance of a public area could indeed raise Fourth Amendment concerns after *Carpenter*. First, in *People v. Tafoya,*[256] the Colorado Court of Appeals ruled that police violated the Fourth Amendment when they used a utility pole-mounted video camera to spy into Tafoya's backyard continuously for three months, and reversed Tafoya's conviction.[257] Acting on a tip, the police believed Tafoya's home was a possible drug "stage house" and, without a warrant, police installed a camera on a utility pole across the street from Tafoya's house. [258] Detectives watched live and recorded footage from Tafoya's property via a camera with zooming and panning capabilities.[259] The officers secured a search warrant only after seeing video showing another man coming to the home and then carrying off plastic bags which were later found to contain methamphetamine and cocaine.[260]

The Court of Appeals rejected the state's argument that the video surveillance was not a search because Tafoya's property could also have been seen through a gap in the fence by any person on the sidewalk or by a neighbor in the stairway of a nearby apartment.[261] Certainly video footage was much more efficient than human surveillance because: (1) it was unlikely that any pedestrian or neighbor for three months would peer through a gap in a six-foot privacy fence or stand on his or her outdoor stairway, and (2) it is equally improbable that someone would watch in a helicopter or watch a camera installed on a drone.[262] The court stressed the duration of the monitoring as especially relevant to the issue of whether police have engaged in a "search." It referred to the *Jones* concurrence and *Carpenter*, when it acknowledged that just because a citizen's

252. *Id.*
253. *See* Slobogin, *supra* note 245, at 289.
254. *Id.*
255. *See e.g.,* California v. Ciraolo, 476 U.S. 207 (1986); Florida v. Riley, 488 U.S. 445, 448–55 (1989); United States v. Bucci, 582 F.3d 108, 116–117 (1st Cir. 2009); Henderson v. People, 879 P.2d 393, 387 (Colo. 1994).
256. No. 17CA1243, 2019 Colo. App. WL 6333762.
257. *Id.* at 29.
258. *Id.* at 1–2.
259. *Id.* at 1.
260. *Id.* at 5.
261. *Id.* at 25.
262. *Id.*

actions were otherwise observable by the public at large does not foreclose a finding of a "search."[263]

Second, the Massachusetts Supreme Court in *Commonwealth v. Mora*[264] concluded that the continuous long-term police surveillance through five hidden police video cameras with real-time zoom capabilities on public telephone and electrical poles was a violation of the Fourth Amendment of the U.S. Constitution and Art. 14 of the Massachusetts Declaration of Rights.[265] These cameras, aimed at two residences, recorded uninterruptedly, twenty-four hours a day, seven days a week, for a few months.[266] The court rejected the Commonwealth's contention that the absence of fencing or other efforts to shield the residences from view showed that the defendants did not have a subjective expectation of privacy in those areas.[267] On the contrary, the court concluded that the defendants did not expect to be surveilled coming and going from their homes over an extended period of time.[268] The court noted that targeted long-term pole camera surveillance of the area surrounding a residence has the capacity to invade the security of the home, and it is even more revealing than CSLI or GPS person tracking.[269] It considered the prolonged and targeted pole camera surveillance of a home as having the potential to generate far more data regarding a person's private life—"[t]he longer the surveillance goes on, the more the boundary between that which is kept private, and that which is exposed to the public, is eroded."[270]

Reminiscent of the reasoning in *Tafoya,* the court was not swayed by the Commonwealth's argument that the video surveillance was merely a substitute for human surveillance in this drug case.[271] As a depository for data, camera surveillance offers a far richer profile of the defendant's life than human surveillance: "[u]nlike a police officer, a pole camera does not need to eat or sleep, nor does it have family or professional concerns to pull its gaze away from its target . . . [t]hus, the pole cameras allowed investigators to overcome several practical challenges to pervasive human surveillance."[272]

But in a third case, *United States v. Moore-Bush*,[273] the First Circuit took a different approach when it reversed the district court's order suppressing evidence obtained from a pole camera.[274] Without a warrant, the Bureau of Alcohol, Tobacco, Firearms, and Explosives placed a camera on a utility pole

263. *Id.* at 20–21.
264. 485 Mass. 360, 361 (Mass. 2020).
265. *Id.*
266. *Id.* at 362.
267. *Id.* at 366–67.
268. *Id.* at 368–69.
269. *Id.* at 370.
270. *Id.* at 373.
271. *Id.* at 374.
272. *Id.*
273. 963 F.3d 29, 31 (1st Cir. 2020).
274. *Id.* at 47.

across the street from the suspect's house in an unlawful firearms sales investigation.[275] The camera with panning, tilting, and zooming abilities was used 24/7 for eight months to surveil the driveway and the front of the house.[276] Law enforcement officers monitored a live feed and recorded footage of the front side of the house, the front of the side door, the attached garage, the driveway, sections of the lawn, and a portion of the public street in front of the house.[277]

In the majority panel's view, *Carpenter* provided no basis for departing from precedent. The majority panel stressed that the pole camera was a standard security camera which the government was allowed under the public-view doctrine, and made this distinction:

> "[P]ole cameras are plainly not an equivalent to CSLI. The pole camera here captured only a small slice of the daily lives of any residents, and then only when they were in particular locations outside and in full view of the public. Pole cameras are fixed in place and do not move with the person as do cell phones generating CSLI . . . [T]his pole camera captured less information about the defendants than someone on the street could have seen and captured."[278]

However, in concurrence, Judge Barron disagreed with the leading opinion's view that *Carpenter's* caveat—that excluded conventional surveillance techniques and tools from its holding—should affect the analysis.[279] To Barron, a "security camera" differs from a pole camera: "[c]onventional 'security cameras' are typically deployed by property owners to keep watch over their own surroundings, not as a law enforcement tool for conducting a criminal investigation by peering into property owned by others."[280] Barron posited, "I cannot see how *Carpenter* may be read to go even a step further and to hold—by virtue of its reference to "security cameras"—that the months-long, uninterrupted video surveillance of the activities surrounding one's home by law enforcement invades no privacy expectation that society should be prepared to accept."[281]

Certainly, all of these vigorous arguments as to whether the Fourth Amendment requires a warrant for placing a pole camera outside of someone's home will be revisited soon as the First Circuit has granted *en banc* review of *Moore-Bush*.[282] Meanwhile, if nothing else, these recent rulings are reminders that Fourth Amendment jurisprudence in technology surveillance cases remains in flux, and what constitutes a search continues to be a subject of debate amongst jurists.

---

275. *Id.* at 46.
276. *Id.* at 32–33.
277. *Id.*
278. *Id.* at 42.
279. *Id.* at 49 (Barron, J., concurring).
280. *Id.* at 57.
281. *Id.* at 52.
282. *United States v. Moore-Bush*, U.S. Court of Appeals, First Circuit, No. 19-1582, Order of the Court (Dec. 9, 2020).

B. Stingray Cell-Site Simulators and Facial Recognition and Facial Surveillance Technology

Noticeably, there is limited to non-existent coverage of Stingray cell-site simulators in both Rise *of Big Data Policing* and *Smart Surveillance*. Ferguson limits his discussion of cell-site surveillance to two paragraphs and Simmons avoids it completely.[283] This is unfortunate because Stingrays exemplify how far law enforcement will go to spy on their unsuspecting targets. Stingrays are the military grade cell-site simulators used by federal and local law enforcement in the past decade to electronically track individuals suspected of criminal activity, or to conduct mass surveillance on groups of unsuspecting people or particular areas.[284] Stingrays directly capture texts, numbers of outgoing calls, emails, serial numbers, identification, GPS location, actual content of conversation, and other raw and detailed information from nearby phones and track the location of targets and non-targets in apartments, cars, buses, and on streets through mapping software. They can even make the tracked device send texts and make calls.[285]

Although there are legitimate uses of Stingrays in tracking down dangerous fugitives, Stingrays are used more commonly as a tracking device for locating stolen cell phones or scanning from the skies over amusement parks and along the border.[286] Absent any specified protocol about their Stingray use or judicial oversight, law enforcement freely relies on Stingrays to target particular individual protesters or to mass collect phone numbers in high-crime areas.[287]

---

283. *See* FERGUSON, *supra* note 7, at 109–10.

284. *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.

285. *See, e.g.,* Andrew Hemmer, *Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches*, 91 CHICAGO-KENT L. REV. 295, 296–97 (2016) (describing the tracking abilities of Stingrays and how they can "hijack" a phone to perform calls and texts disguised as the targeted phones); FRIEDMAN, *supra* note 9, at 262 (same); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 145 (2013) (same); Austin McCullough, *StingRay Searches and the Fourth Amendment Implications of Modern Cellular Surveillance*, 53 AM. CRIM. L. REV. ONLINE 41, 41 (2016) (same). The collateral consequences resulting from their use include the disruption of cell service to phones in the form of service outages, blocked and dropped calls, and causing a connected cell phone's battery to drain and die. *See* Brian Barrett, *The Baltimore PD's Race Bias Extends to High-Tech Spying, Too*, WIRED (Aug. 16, 2016), 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), https://mashable.com/2016/10/03/police-technology-surveillance-racial-bias/; Marlan Hetherly, *Judge Rules Surveillance Info Collected by Police Stingrays Can Remain Confidential*, WBFO NPR (Apr. 12, 2018), http://news.wbfo.org/post/judge-rules-surveillance-info-collected-police-stingrays-can-remain-confidential.

286. *See* George Joseph, *Racial Disparities in Police "Stingray" Surveillance, Mapped*, BLOOMBERG (Oct. 18, 2016), https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-sureveillance-mapped/502715/.

287. *See* Klonick, *supra* note 5; *see also* Andrew Guthrie Ferguson, *The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment*

When challenged, the government's reluctance, and sometimes outright refusal, to provide the courts with information about the capabilities of Stingrays and similar technology evokes great skepticism about their legitimacy and efficiency.[288] Understandably, there has been mounting outcry at the grassroots level against Stingray surveillance by public defenders and privacy activists who are demanding that police be more transparent about the surveillance and that the public be allowed to participate in the decision-making process over how Stingrays are used.[289] Arizona, California, Colorado, Florida, Illinois, Indiana, Maine, Maryland, Minnesota, Missouri, Montana, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin have passed laws that protect citizens' cell phone data and which require police to get a warrant to use a Stingray.[290]

Next, facial recognition and facial surveillance technology are the latest threats to associational privacy and personal security, but only make cameo appearances in the volumes.[291] Even though Ferguson covers these police

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).

288. *See* Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 The FEDERALIST SOC'Y REV. 29, 32 (2016) (reporting on speculation by commentators state and federal charges have been reduced or dismissed by federal prosecutors in lieu of having to give confidential information about Stingrays to the court); Mike Maharrey, *Federal Programs are Funding Local Stingray Spying*, TENTH AMENDMENT CENTER (Aug. 26, 2017), https://tenthamendmentcenter.com/2017/08/26/federal-programs-are-funding-local-stingray-spying/.

289. *See* George Joseph, *Racial Disparities in Police "Stingray" Surveillance, Mapped*, BLOOMBERG (Oct. 18, 2016), https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-sureveillance-mapped/502715/.

290. *See, e.g.*, Katherine M. Sullivan, *Is Your Smartphone Conversation Private? The StingRay Device's Impact on Privacy in States*, 67 CATH. U.L. REV. 388 (2018) (arguing for more state legislation to protect privacy of citizens); Cox, *supra* note 288, at 17 (discussing the reaction by various state legislatures to the use of Stingrays and remarking "[T]welve states have passed laws mandating law enforcement use of a cell-site simulator must be based upon a court issued search warrant based upon a finding of probable cause"); Mike Maharrey, *Arizona Bill Would Prohibit Warrantless Stingray Spying, Hinder Federal Surveillance Program*, TENTH AMENDMENT CENTER (Feb. 7, 2017), https://fromthetrenchesworldreport.com/arizona-committee-passes-bill-prohibit-warrantless-stingray-spying/182520; Klonick, *supra* note 5; 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/; Michael Maharrey, *Florida Committee Passes Bill to Limit Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMENDMENT CENTER (Jan. 27, 2021), https://blog.tenthamendmentcenter.com/2021/01/florida-committee-passes-bill-to-limit-warrantless-stingray-spying-help-hinder-federal-surveillance/; Robert Snell, *Feds Use Anti-Terror Tool to Hunt the Undocumented*, DETROIT NEWS (May 19, 2017), https://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/ (offering that States can adopt laws requiring judicial authorization before local law enforcement is allowed to use Stingrays and limiting on how long they can retain the data and reserve their use only in cases implicating violence or harm to human life).

291. *See Facial Recognition Technology: (Part I) Its Impact on our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. 5–7 (2019) (written

surveillance tools in much more detail than Simmons, their collective analysis is still relatively limited. These two distinct kinds of technology are not governed by any legislation, and it remains an open question as to whether the use of such technology by law enforcement constitutes a search for the purposes of the Fourth Amendment.[292]

As an investigative tool, face recognition systems use computer algorithms to compare data on other face images previously collected and stored in driver's license databases, government identifications records, police bookings of all arrestees (including people who are arrested but never charged or who are found innocent), and social media accounts.[293] Just like their secrecy over Stingrays, law enforcement agencies are offering precious little about their use of facial recognition software. According to media reports, the NYPD uses a facial recognition software known as Dataworks Plus, a system integrator that employs facial recognition algorithms.[294] NYPD cross-references photo images of persons against drivers' license databases.[295] The department also collects images from CCTV, drone cameras, and google images.[296] In 2019, NYPD used facial recognition more than 8,000 times.[297] The city of Detroit employs its controversial Project Green Light mass surveillance system, which allows local businesses, churches, public housing, and other participants to install video camera on their premises and stream real-time video feeds to the Detroit Police Department.[298] The Detroit Police Department also applies facial recognition software to still photos from cameras.[299]

---

statement of Professor Andrew Guthrie Ferguson); Taylor Book, *Recognizing Your Privacy Rights: Facial Recognition Technology and Third Party Doctrine*, MICH. TECH. L. REV. (2019), http://mttlr.org/2019/04/recognizing-your-privacy-rights-facial-recognition-technology-and-third-party-doctrine/.

292. There is hope that courts will find facial recognition technology must respect the right to privacy, including a recent case that may offer insight for future facial recognition cases. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1264 (9th Cir. 2019) (ruling that Facebook users in Illinois can move forward in suing the company over facial recognition technology. It was the first federal circuit decision to directly address privacy concerns about facial recognition technology. The case concerned Facebook users in Illinois who accused Facebook of violating the State's Biometric Information Privacy Act, designed to safeguard their privacy). *See generally*, Biometric Information Privacy Act (BIPA), 2007 Ill. Laws 994 (2008).

293. *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, ABA – CRIM. JUST. MAG. (Spring 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

294. *See* Alex Hodor-Lee, *The Blurred Faces—And Ethics—of Protest Photography*, DOCUMENT JOURNAL (June 23, 2020), https://www.documentjournal.com/2020/06/the-blurred-faces-and-ethics-of-protest-photography/.

295. *Id.*

296. *Id.*

297. *See id.*

298. *See* Vince Carducci, *Detroit's Project Green Light and the "New Jim Code*," PUBLIC SEMINAR (Oct. 1, 2020), https://publicseminar.org/essays/detroits-project-green-light/.

299. *See* Kate Kaye, *Privacy Concerns Still Loom Over Detroit's Project Green Light*, SMART CITIES DIVE (Feb. 1, 2021), https://www.smartcitiesdive.com/news/privacy-concerns-still-loom-over-detroits-project-green-light/594230/.

Increased media attention on these systems has illuminated their manifold problems. The National Institute of Standards and Technology's negative performance review of facial recognition technology is one of the largest examinations of facial recognition technology.[300] The agency culled through 18 million photos from mugshots, passports, and travel databases, tested 189 facial recognition algorithms, and concluded that facial recognition programs are racially biased because they erroneously identity the faces of African Americans, Asians, and Native Americans 10 to 100 times more than white faces.[301]

As for a specific case of misidentification, consider the wrongful arrest of Robert Julian-Borchak Williams based on a false match by a recognition algorithm. Two Detroit Police Department Officers arrived at his driveway and handcuffed him in front of his wife and two young children based on a felony warrant for allegedly shoplifting five watches from an upscale boutique.[302] Attached to the warrant was the blurry photo obtained from the store security camera relied upon by the arresting officers.[303] That photo was cross-referenced through a facial recognition software to match with Williams's state-issued drivers' license.[304] Both Williams and the man in the store photo were African Americans.[305] Williams was processed and held overnight at a detention center before he was released on bail.[306]

Following publicity over Williams's case, including coverage in a segment on *60 Minutes*, Democratic lawmakers, amid continued concerns over abuses of facial recognition technology by the government, introduced the Facial Recognition and Biometric Technology Moratorium Act of 2020—the first comprehensive ban on the use of facial recognition technologies by federal agencies.[307] As a sponsor of the legislation, Representative Pramila Jayapal

300. *See* Natasha Singer, *Many Facial-Recognition Systems Are Biased Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

301. *See id.*

302. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *see also* Bobby Allyn, *"The Computer Got It Wrong": How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

303. *See id*.

304. *Id.*

305. *See id*; *see also* Joy Buolamwini, *How Does Facial Recognition Software See Skin Color?*, NPR (Jan. 26, 2018), https://www.npr.org/transcripts/580619086.

306. Hill, *supra* note 302.

307. Thomas Macaulay, *Democrats and Civil Liberties Groups Back Law Banning Facial Recognition Across the US*, THE NEXT WEB (June 26, 2020), *available at* https://thenextweb.com/neural/2020/06/26/democrats-and-civil-liberties-groups-back-law-banning-facial-recognition-across-the-us/.

remarked, "Our legislation will not only protect civil liberties but it will aggressively fight back against racial injustice."[308]

There is also movement against facial recognition at the state level. The California Consumer Privacy Act (CCPA), is the most expansive state privacy law in the United States.[309] The CCPA includes biometric information (facial recognition) within the definition of personal information.[310] Since then, at least six state legislatures have introduced privacy laws similar to the CCPA.[311] In New York, the Public Oversight Surveillance Technology (POST Act) compels NYPD to explain how it uses facial recognition tools and other surveillance technologies to strategically track New Yorkers.[312]

The lawmakers' concerns and foresight are supported by research. The Georgetown Center on Privacy and Technology (hereinafter "the Center") published extensive reports concluding that facial recognition technology is plagued with issues and concerns including: (1) the wide variety of images that police can submit to face recognition algorithms to start investigation leads, and the variety of sources from which they can pull images;[313] (2) law enforcement agencies' failure to check their facial recognition systems for accuracy;[314] (3) a majority of face recognition systems are not audited for misuse;[315] (4) police face recognition disproportionately affects African Americans, women, and senior citizens;[316] and (5) face surveillance may have a chilling effect on our First Amendment rights to free speech and peaceful assembly at public gatherings.[317] The Center recommended a moratorium on the use of face recognition.[318] The

308. *See* Aaron Boyd, *Lawmakers Introduce Bill to Ban Federal Use of Facial Recognition Tech*, NEXTGOV, (June 26, 2020), https://www.nextgov.com/emerging-tech/2020/06/lawmakers-introduce-bill-ban-federal-use-facial-recognition-tech/166489/; Macaulay, *supra* note 307.

309. *See* Joseph J. Lazzarotti & Jason C. Gavejian, *State Law Developments in Consumer Privacy*, 9 NAT'L L. REV (2019).

310. *See* Shaun Moore, *CCPA and Face Recognition to Ensure Personal Privacy*, BIOMETRIC UPDATE (Mar. 9, 2020), *available at* https://www.biometricupdate.com/202003/ccpa-and-face-recognition-to-ensure-personal-privacy.

311. Lazzarotti, *supra* note 309.

312. *See* David Brand, *New City Law Compels NYPD to Explain Surveillance Tools and Strategies*, QUEENS DAILY EAGLE (July 16, 2020), https://queenseagle.com/all/new-city-law-compels-nypd-to-See-surveillance-tools-and-strategies.

313. *See* Clare Garvie, et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, THE GEORGETOWN CENTER ON PRIVACY AND TECHNOLOGY, (2016), https://www.perpetuallineup.org/.

314. *Id*.

315. *Id*.

316. *Id.*; *see also* Jake Laperruque, *Facial Recognition Surveillance Faces New Calls for Legal Limits*, PROJECT ON GOV'T OVERSIGHT (Mar. 13, 2019), https://www.pogo.org/analysis/2019/03/facial-recognition-surveillance-faces-new-calls-for-legal-limits/; Devlin Brown*, Researchers Call Racial Recognition 'Imperfect'*, USA TODAY (Sept. 9, 2019) (reporting higher error rates on the face of people with darker skin relative to those with lighter skin).

317. *See* Clare Garvie & Laura M. Moy, *America Under Watch—Face Surveillance in the United States*, THE GEORGETOWN CENTER ON PRIVACY AND TECHNOLOGY (May 16, 2019), https://www.americaunderwatch.com/.

318. *Id.*

Center further recommended that state legislatures pass commonsense legislation to comprehensively regulate facial recognition technology, including requiring reasonable suspicion of criminal conduct prior to a face recognition search.[319]

Facial surveillance technology is equally problematic because it casts such a wide net. Street surveillance cameras and police-worn body cameras indiscriminately search all faces–all looking from different distances, varied angles, and different lighting–against a search list.[320] Real-time facial recognition software linked to video surveillance cameras and biometric databases checks a person for active warrants, assesses risk level, and monitors prior locations at particular times through citywide surveillance images.[321] As with CSLI and Stingrays, this real-time tracking of individual's movement over an extended period of time could reveal intimate details about the individual's personal life.[322]

The controversy over facial recognition has done little to dissuade local police from scanning surveillance footage from third-party platforms to identify faces or from data mining stored images that contain revealing meta data from third-party platforms, such as Facebook, Google, Instagram, Twitter, and YouTube, to identify persons.[323] More dubious is Clearview AI's new groundbreaking facial recognition app, Smartcheckr, used by the FBI, the Department of Homeland Security, and over 600 law enforcement agencies.[324] Akin to a Google search, the app allows a sensitive photo of a person to be uploaded to match public photos of that person, and offer links to where those photos appeared in just seconds.[325] Astonishingly, Smartcheckr has a database of more than three billion images scraped from Facebook, Youtube, and millions of other websites.[326] Police can also upload photos and videos taken from a

319. Garvie et al., *supra* note 317.

320. *See* Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELECTRONIC FRONTIER FOUNDATION (Feb. 12, 2018), *available at* https://www.eff.org/wp/law-enforcement-use-face-recognition.

321. *Id*.

322. *Facial Recognition Technology: (Part I) Its Implication On Our Civil Rights and Liberties, Hearing Before the H.R. Comm. on Oversight and Reform*, 116 Cong. 7, 18 (2019) (statement of Andrew G. Ferguson); *see* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?,* AMERICAN BAR ASSOCIATION (2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

323. *See e.g.*, Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020); *see also* Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/; *see also* Russell Brandom, *Can Facebook and Twitter Stop Social Media Surveillance?*, THE VERGE (Oct. 12, 2016), https://www.theverge.com/2016/10/12/13257080/police-surveillance-facebook-twitter-instagram-geofeedia.

324. Hill, *supra* note 323.

325. *Id*.

326. *Id.*

bystander's phone.[327] Additional unease is found in Clearview AI's ability to store all uploaded content and manipulate results.[328] Although law enforcement agencies attest to the Smartcheckr's effectiveness, this relatively new app has yet to be independently checked for accuracy by the National Institute of Standards and Technology or anyone else.[329]

Clearview AI faces tremendous backlash. The American Civil Liberties Union filed suit against Clearview for violating the Illinois Biometric Information Privacy Act for illegally collecting and storing data on Illinois citizens without their knowledge or consent and selling that access to law enforcement and private companies.[330] The Vermont Attorney General has also sued Clearview to prohibit the company from collecting Vermonters' photos and facial recognition data, and YouTube, Facebook, LinkedIn, and Twitter Tech sent cease and desist orders to stop Clearview from scraping their site's images and information.[331]

Last summer, SFPD received real-time live access to hundreds of business' district cameras, along with an indiscriminate "data dump" of over a week's worth of camera footage amid the ongoing demonstrations against police violence.[332] In response, the ACLU of California and the Electronic Frontier Foundation filed a civil rights lawsuit on the behalf of African American and Latinx protesters against the city of San Francisco seeking declaratory relief and an injunction for violating San Francisco's Surveillance Technology Ordinance[333] by using a private network of more than 400 surveillance cameras to spy on protestors in real-time.[334] The Ordinance requires approval from the city's Board of Supervisor to acquire and use new surveillance technology, and the complaint alleges that SFPD failed to do this.[335] SFPD's tracking of BLM protesters was not the first time the police circumvented the city's facial recognition technology ban. In a recent case, SFPD posted a photo taken from a surveillance camera in a crime-alert bulletin when it needed help in locating a

327. *Id.*

328. *Id*.

329. *Id*.

330. *See* Nick Statt, *ACLU Sues Facial Recognition Firm Clearview AI, Calling It a 'Nightmare Scenario' for Privacy*, THE VERGE (May 28, 2020), https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws.

331. *See* Jon Porty, *Vermont Attorney General is Suing Clearview AI Over Its Controversial Facial Recognition App*, THE VERGE (Mar. 11, 2020), https://www.theverge.com/2020/3/11/21174613/clearview-ai-sued-vermont-attorney-general-facial-recognition-app-database.

332. Guariglia et al., *supra* note 3.

333. S.F. Admin. Code § 19B (2019).

334. *See* Daniel Moattar, *SF Tech Moguls Funded the Cameras. Cops Used Them to Spy on Protesters*, MOTHER JONES (Oct. 7. 2020), https://www.motherjones.com/anti-racism-police-protest/2020/10/sf-tech-moguls-funded-the-cameras-cops-used-them-to-spy-on-protesters/.

335. Complaint for Declaratory and Injunctive Relief, *Reyes v. City and Cnty. of S.F.*, No. CGC-20-587008 at 2 (Oct. 2020) (on file with the author).

suspect.[336] That call was answered by the Northern California Regional Intelligence Center after it applied facial recognition technology to find a match in its photo database[337]

Amidst the BLM protests against police brutality on the opposite coast, NYPD detectives used face recognition and comparison technology, along with footage from the public, to apprehend and arrest suspects engaged in criminal activity.[338] The NYPD also paired up with the FBI's High Intensity Drug Trafficking Area program to merge the NYPD's biometric repository with the FBI databases.[339] Apparently, the widespread use of face masks to avoid the spread of COVID-19 was not slowing down some facial recognition expansion despite the risk of errors leading to wrongful arrests. Responding to concerns that protective masks make facial recognition systems–including video imaging processing hardware and software and image recognition algorithms–less effective, some companies updated their algorithms by photoshopping masks onto images.[340]

At the same moment, some other tech companies stood in solidarity with the BLM movement. IBM stopped development of its face recognition system and has reconsidered police sales altogether.[341] Amazon and Microsoft announced they would not sell facial recognition products and services to local law enforcement but were silent as to sales to the federal government.[342]

CONCLUSION

As companion books, *Rise of Big Data Policing* and *Smart Surveillance* engage in an important dialogue about the growth of new technologies and how citizens, legislators, the police, and the court system need to work together to advance Fourth Amendment jurisprudence so that our civil liberties are protected. As this Review has vividly shown, the benefits of having public surveillance are significantly outweighed by the government's abuse of surveillance technology and the corresponding reduction in our reasonable expectation of privacy under the Fourth Amendment. As the national conversation about racial justice continues, more accountability and

336. *See* Megan Cassidy, *Facial Recognition Tech Used to Build SFPD Gun Case, Despite City Ban*, S.F. CHRONICLE (Sept. 24, 2020), https://www.sfchronicle.com/bayarea/article/Facial-recognition-tech-used-to-build-SFPD-gun-15595796.php.

337. *See id.*

338. *See* Hodor-Lee, *supra* note 294.

339. *Id*.

340. *See* Sam Biddle & Mara Hvistendahl, *Homeland Security Worries Covid-19 Masks Are Breaking Facial Recognition, Leaked Document Shows*, THE INTERCEPT (July 16, 2020), *available at* https://theintercept.com/2020/07/16/face-masks-facial-recognition-dhs-blueleaks/.

341. *See* Matt Cagle, *Microsoft Says It Supports Racial Justice. Will It Refuse to Power Discriminatory Police Surveillance?*, ACLU (June 10, 2020), *available at* https://www.aclu.org/news/privacy-technology/microsoft-says-it-supports-racial-justice-will-they-refuse-to-power-discriminatory-police-surveillance/.

342. *See id.*

transparency on the part of the police, the courts, and legislators are desperately needed. States and cities should continue to pass laws that require regulation of police acquisition and the use of surveillance technology. The surveillance state is here.