Seattle Journal for Social Justice

Volume 21 | Issue 2 Article 13

2023

Crim Pro Rewired: Why Current Police Practices Require Candor in the Classroom

Elizabeth N. Jones

Crim Pro, Rewired: Why Current Police Practices Require Candor in the Classroom

Elizabeth N. Jones*

Police today use powerful digital surveillance to investigate crime, and then store and share the bulk data collected with virtually no restraint. My future Criminal Procedure classes need a rewired approach.

INTRODUCTION

Law students in Constitutional Criminal Procedure courses immediately confront the many "zigs and zags" of Fourth Amendment jurisprudence.[1] They will find little comfort in learning that these turbulent times are the subject of great academic thought.[2] Students cringe when professors answer questions with the standard "it depends," so ambiguity of this magnitude will surely cause alarm. They will understand why there is confusion, but they will not enjoy the chaos.

Current uncertainty in the law aside, there is a lot to like about Criminal Procedure. It is the most practical, the most significant, and really, the most interesting doctrinal material law students encounter. It may seem bold to

* Professor of Law, Western State College of Law.

[1] JOSHUA DRESSLER ET AL., CRIMINAL PROCEDURE: INVESTIGATING CRIME 68 (West Acad. Publ., 7th ed., 2020) (analogizing the study of Criminal Procedure to following a path with "many significant turns, including some U-turns, as well as zigs and zags").

[2] *See generally* Barry Friedman & Cynthia Benin Stein, *Redefining What's 'Reasonable:' The Protections for Policing*, 84 GEO. WASH L. REV. 281 (Mar. 2016); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014); Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67 (2013); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357 (2018); Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012); Rachel Levinson Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L. J. 527 (2017).

make such hyperbolic claims about a law school course, but that boldness is borne out. Criminal procedure is practical and significant because the law of police investigations—what the police can and cannot do when investigating a crime—affects every single encounter students will have with law enforcement. Indeed, everyone should be familiar with this constitutional subject matter; since people never know if or when they will interact with the police, it is wise to examine the legalities of police procedures before such encounters occur. What does it mean to be "detained" by the police? When can an officer look inside a student's backpack? Does it matter if the student is on a sidewalk, or in a car, or in a house? Understanding the law may mean the difference between a "not guilty" or "guilty" verdict, and even between life and death itself. That criminal procedure is interesting—a somewhat subjective position, to be sure—can be evidenced by the multitude of entertainment industry projects centered around the criminal justice system.[3]

Whether offered as an upper-level elective or first-year requirement, constitutional criminal procedure courses invariably begin with the Fourth Amendment.[4] Students critically analyze the black letter words and

[3] *See, e.g.*, Alissa Wilkinson, *9 Movies and Shows That Explain How America's Justice System Got This Way*, VOX, (June 1, 2020, 3:40 PM), https://www.vox.com/culture/2020/6/1/21276965/policing-prisons-movies-shows-streaming-netflix [https://perma.cc/GS4A-UY9C]; David Reddish, *15 Movies to Make You Question the Criminal Justice System*, SCREENRANT, (June 30, 2016), https://screenrant.com/movies-make-you-question-criminal-justice/ [https://perma.cc/P69X-84CS]. The popularity of "true crime" television and podcasts also point to interest in police procedures. *See, e.g.*, John Koblin, *Mystery Solved: 'Dateline' Finds Path from TV to Podcast Stardom*, N.Y. TIMES, (Oct. 2, 2022), https://www.nytimes.com/2022/10/02/business/media/dateline-podcast-true-crime.html [https://perma.cc/825M-LZW9].

[4] *ABA Standards and Rules of Procedure for Approval of Law Schools 2021–2022*, 2021 A.B.A. SECTION ON LEGAL EDUC. AND ADMISSIONS TO THE BAR 17, https://www.americanbar.org/content/dam/aba/administrative/legal_education_and_admissions_to_the_bar/standards/2021-2022/2021-2022-aba-standards-and-rules-of-procedure-chapter-3.pdf [https://perma.cc/7PNC-3NLE], (301(a) requires ABA-accredited law schools to ". . . maintain a rigorous program of legal education that

underlying policies of the Fourth Amendment, and how those words and policies have been construed by courts, up to and including the final arbiter of case precedent, the United States Supreme Court. Regaling students with courtroom war stories won't meet most "best practice" standards of teaching, but nonetheless students do seem to appreciate professors' "real life" work experience in the classroom. Students more meaningfully understand and retain information when they can relate it to how it is used in "real life" situations.[5] And hopefully the inverse is also true, because my students are about to find out that the way police apply the law today does not always resemble the laws and rules they are learning about in class.

As a criminal defense attorney, the Fourth Amendment was a means to an end and the first building block behind the case law supporting my arguments. A written motion to suppress evidence would address the Constitution as an introductory matter, but actually invoking the Fourth Amendment in an argument to the court would probably verge on the overdramatic. Now, as a law professor, presenting the Fourth Amendment to a new group of Crim Pro students is an exciting, almost passionate undertaking.

The Fourth Amendment represents the government's promise to protect its people from unjust intrusions and indiscriminate meddling. It states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

prepares its students, upon graduation, for admission to the bar and for effective, ethical, and responsible participation as members of the legal profession.").

[5] *See generally* Tonya Kowalski, *True North: Navigating for the Transfer of Learning in Legal Education*, 34 SEATTLE UNIV. L. REV. 51, 70 (2010) (explaining and comparing cognitive learning theories for law students); Jordan Rothman, *Law Professors Should Have More Practical Experience*, ABOVE THE LAW (Aug. 26, 2020, 11:21 AM), https://abovethelaw.com/2020/08/law-professors-should-have-more-practical-experience/ [https://perma.cc/5M3L-GUA5] (noting the lack of fulltime law professors with courtroom experience and the accompanying "practical tips to provide in their lectures" contributed to a "less meaningful" law school experience for the author).

> probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[6]

These fifty-four words acknowledge the sanctity of one's living space, the need for judicial oversight to ensure governmental restraint, and the value in balancing the desires of each individual with the demands of society as a whole. It is the framework of the American criminal justice system and the foundational starting point for the enforcement of criminal law and order.

At its core, the Fourth Amendment is intended to restrain governmental overreach by limiting its conduct to that which is reasonable. The Fourth Amendment warrant requirement has withstood over two centuries of judicial interpretation, ideological party differences, and vast social change. And while technological innovations emerge frequently and with varying degrees of fanfare, this time it is different.

Highly sophisticated, digitalized equipment has completely transformed how law enforcement investigates nearly every type of crime at every level of authority. Police departments today use body-worn cameras[7] and face recognition systems.[8] They have access to automatic license plate readers[9]

---

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

[7] *Research on Body-Worn Cameras and Law Enforcement*, NAT'L INST. JUST. (Jan. 7, 2022), https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement [https://perma.cc/LY7J-7JFY] (finding that 80% of large police departments in the United States had acquired body-worn cameras by 2016).

[8] Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS INST. (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/56HL-MZPN] (noting that facial recognition is a common tool for law enforcement, but that after protests over George Floyd's murder in 2020 some companies such as Amazon and Microsoft agreed to stop selling this technology to law enforcement).

[9] Lauren Fash, *Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy*, 78 MD. L. REV. ONLINE 63, 65 (2019) (noting that "the majority of police departments in the United States use [ALPR] devices" and discussing some concerns associated with this form of police surveillance).

and acoustic gunshot sensors[10] and pole cameras[11] and software that can monitor social media[12] and mobile device forensic tools to extract raw and metadata from cellphones.[13] They employ drones[14] and international mobile subscriber identity-catchers.[15]

A plethora of police tech, in itself, is not the problem.[16] Sweeping surveillance technology has brought some benefit to society. For example,

---

[10] Jon Schuppe & Joshua Eaton, *How ShotSpotter Fights Criticism and Leverages Federal Cash to Win Police Contracts*, NBC NEWS (Feb. 10, 2022, 6:39 AM), https://www.nbcnews.com/news/us-news/shotspotter-police-gunshot-technology-federal-grants-rcna13815 [https://perma.cc/2MG4-GMHK] (discussing problems with technology from ShotSpotter, a publicly traded company providing "gunfire finding" tech to "about 120 police departments" across the United States).

[11] Sara Merken, *7th Circ. Sides with Gov't in Pole Camera Surveillance Case*, REUTERS (July 14, 2021, 3:16 PM), https://www.reuters.com/legal/government/7th-circ-sides-with-govt-pole-camera-surveillance-case-2021-07-14/ [https://perma.cc/JDS7-XGKD] (recounting the use of pole cameras in United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021), *cert. denied*, 212 L. Ed. 2d 7, 142 S. Ct. 1107 (2022)).

[12] Mary Pat Dwyer, *LAPD Documents Reveal Use of Social Media Monitoring Tools*, BRENNAN CTR. JUST. (Sept. 8, 2021), https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-reveal-use-social-media-monitoring-tools [https://perma.cc/ZWL4-DMYP].

[13] Sidney Fussell, *How Police Can Crack Locked Phones—and Extract Information*, WIRED (Oct. 23, 2020, 7:00 AM), https://www.wired.com/story/how-police-crack-locked-phones-extract-information/ [https://perma.cc/E92K-GWAL] (noting a research nonprofit company's report finding that police departments in every state contract with digital forensic vendors to "access and copy data from locked phones").

[14] Ben Brazil, *Civil Libertarians Raise Concerns as O.C. Sheriff's Department Prepares to Launch Drone Program*, L.A. TIMES (Apr. 12, 2019, 11:37 AM), https://www.latimes.com/socal/daily-pilot/news/tn-wknd-et-drones-orange-county-sheriff-department-20190412-story.html [https://perma.cc/7BG6-M6KP] (comparing the Sheriff's Departments' drone programs in Orange County (5 drones, 24 pilots) with San Diego (12 drones, 19 pilots) and Los Angeles (1 drone, 6 pilots)).

[15] Matt Cagle, *Dirtbox Over Disneyland? New Docs Reveal Anaheim's Cellular Surveillance Arsenal*, VOICE OF OC (Jan. 27, 2016) https://voiceofoc.org/2016/01/aclu-dirtbox-over-disneyland-anaheims-cell-surveillance-arsenal-revealed/ [https://perma.cc/AYB3-WGRS] (describing "powerful cell phone surveillance devices" purchased by the Anaheim Police Department and revealed as the result of an ACLU FOIA request).

[16] Dave Davies, *Surveillance and Local Police: How Technology is Evolving Faster than Regulation*, NPR (Jan. 27, 2021, 12:51 PM), https://www.npr.org/2021/01/27/961103187/surveillance-and-local-police-how-

GPS trackers and drones can help search crews find lost people.[17] Cell phone apps and location data can assist police in linking separate but similar crimes together.[18] Automatic license plate readers can aid in the recovery of stolen vehicles.[19]

It is concerning, however, that such state-of-the-art technology is already in active use without uniform regulations or enforcement systems in place and, in many instances, without any community buy-in.[20] Police

technology-is-evolving-faster-than-regulation [https://perma.cc/7KAT-5G3R] (noting that "technology is not good or bad in itself").

[17] Audrey McAvoy, *GPS, Special Maps and the Wild: Tech Helps Searchers Zero in on Missing People*, DENVER POST (June 30, 2019, 1:00 PM), https://www.denverpost.com/2019/06/30/gps-maps-searchers-missing-people/ [https://perma.cc/D6XE-KDZM] (describing how GPS coordinates and drones found a hiker lost in a Maui forest for 17 days); *Woman Trapped 14 Hours in Canyon Crash Rescued in Orange County*, ABC7 (May 12, 2016) https://abc7.com/woman-trapped-14-hours-car-crash-embankment-canyon/1336030/ [https://perma.cc/4QX5-NQMA] (quoting the Orange County Fire Authority, "The only way (the California Highway Patrol) found her was because the CHP had pinged her phone and it came back to one of the cellphone [sic] towers in the area . . .").

[18] Casey J. Bastian, *Reverse Location Warrants Neglect Particularity Requirement*, CRIM. LEGAL NEWS (June 2021) (noting that prosecutors find using location data helpful to solve "pattern crimes, such as arson, burglary, or sexual assaults"); *see also*, Thomas Brewster, *Life360 Comes at You Fast—Cops Convince Arson Suspect's Kid to Give Up Dad's Location on Family Tracking App*, FORBES (Feb. 12, 2020), https://www.forbes.com/sites/thomasbrewster/2020/02/12/life360-comes-at-you-fast—cops-use-family-surveillance-app-to-trace-arson-suspect/?sh=6704c5c9380a [https://perma.cc/5XCR-K2XB] (describing how the Life360 app transforms a cell phone into a "mini surveillance device" that can provide "precision location coordinate information" and "specific times the cell phone (is) moving and stationary").

[19] Cody Dulaney, *Police in San Diego County Breaking the Law Sharing Drivers' Data*, INEWSOURCE (Jan. 6, 2022), https://inewsource.org/2022/01/06/police-share-license-plate-data/ [https://perma.cc/3QUC-URGA] (noting that during a six-month period of 2018 Carlsbad police scanned over 48 million license plates and successfully recovered sixty-five vehicles).

[20] *See, e.g.*, Jonathan Hofer & Christopher B. Briggs, *The Rest of America Should Learn from California's Smart-City Missteps*, INDEP. INST. (Nov. 9, 2021), https://www.independent.org/news/article.asp?id=13858 [https://perma.cc/PS6C-KLDZ] (reporting that San Diego County officials failed to tell the public that police were routinely accessing video equipped inside newly installed "Smart Streetlights" to investigate crime); Jennifer A. Kingston, *The Future of "Smart" Cities is in Streetlights*, AXIOS (Feb. 11, 2021), https://www.axios.com/2021/02/11/smart-cities-street-lights

investigative practices have become, to be blunt, a "global free-for-all data collection snoopvertising ecosystem with zero functional oversight."[21] From a pedagogical standpoint, it feels disingenuous to not at least mention law enforcement's embrace of and reliance on invasive mass surveillance to combat crime. Whether debated in a classroom or argued in a courtroom, digital policing is fraught with new, as-of-yet unresolved legal challenges. This essay focuses on three of them.

Part I of this Essay examines whether a new approach is needed to right the balance between our government's omnipresent police surveillance and its cell phone-toting citizenry. It considers the continued viability of two legal tenets: the reasonable expectation of privacy test and the third-party doctrine. Part II of this Essay questions the prolific use of reverse location search warrants and their compliance with Fourth Amendment standards. It analyzes language from actual search warrants and probable cause affidavits to supplement academic rhetoric and classroom reading. Part III of this Essay explores the semi-secretive dynamic between government agencies and third-party tech vendors which enables police to avoid constitutional requirements. With new technologies only reluctantly revealed and only then after court order, it appeals to law students, lawyers, and really anyone with a cell phone to be aware of these unsettled (and unsettling) legal issues.

[https://perma.cc/A6X8-8K5M] (noting community "pushback" to San Diego police use of video from its "Smart Streetlights" program without first informing the public).

[21] Karl Bode, *Marco Rubio Pretends to be a TikTok Privacy Champion, Despite Years of Undermining U.S. Consumer Privacy*, TECHDIRT (July 8, 2022, 6:33 AM), https://www.techdirt.com/2022/07/08/marco-rubio-pretends-to-be-a-tiktok-privacy-champion-despite-years-of-undermining-u-s-consumer-privacy/ [https://perma.cc/754S-93KF] (describing how and why "dodgy adtech, telecoms, or data brokers" collect and sell Americans' user data to foreign governments).

I. COURTS PROBABLY NEED A NEW TEST TO ENSURE CONTINUED FOURTH AMENDMENT PROTECTIONS

Law students are potential criminal justice stakeholders of the future. Within this context, they should recognize some of the many consequences of living in a surveillance state. This includes whether the current "reasonable expectation of privacy" test remains an appropriate measure of Fourth Amendment protection. But before they can take on this task, they will need to get through the basics of Criminal Procedure.

Criminal Procedure begins with a simple yet essential matter: the Fourth Amendment applies to government action.[22] Students then realize that the words of the Fourth Amendment are not always given their plain meaning, and thus interpreting the Fourth Amendment can be an ordeal that is anything but simple. Some historical background helps students connect the Fourth Amendment to judicial case law and then relate that case law to "real life" police work.

For Fourth Amendment purposes, the word "search" is a legal term of art. It was first understood as solely a property-based protection.[23] A "search" required that government officials physically trespass into an area in violation of a landowner's privacy interests.[24] This concept of "privacy" changed with the landmark case of *Katz v. United States*. In *Katz*, government agents physically attached a listening device to the outside of a telephone booth to hear Mr. Katz place illegal sports bets inside the booth.[25] The phone booth allowed people to see inside, but Mr. Katz closed the door

[22] This straightforward principle merited little discussion in the past but, for reasons explained in Part IV, *infra*, should be emphasized in this newly rewired version of Crim Pro.

[23] Olmstead v. United States, 277 U.S. 438 (1928).

[24] *Id.* at 464–65 (reasoning that the Fourth Amendment required the physical trespass of an individual's person, houses, papers, and effects by the government), *overruled by* Berger v. State of N.Y., 388 U.S. 41 (1967), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

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

before placing his call, intending to prevent outside observers from hearing his conversation.[26]

The word "privacy" is not found in the Fourth Amendment itself, but the *Katz* case established the current approach to linking privacy interests and the Fourth Amendment. In *Katz*, the Supreme Court held that police engage in a "search" (and must therefore abide by the Fourth Amendment) if a "reasonable expectation of privacy" in the subject of the search is found to exist.[27] Here, Mr. Katz closed the phone booth door to "exclude . . . the uninvited ear" and was thus "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[28] The government must now obtain a warrant before searching even public places if an expectation of privacy in that place is reasonable.

Crim Pro introductory material includes case law which explains the strong preference for police to obtain warrants as an assurance of "the lawful authority of the executing officer . . . and the limits of his power."[29] Students learn that warrants are issued by a "neutral and detached magistrate" as a measure of oversight to the police, who are "engaged in the often-competitive enterprise of ferreting out crime."[30] And students also learn that police need not obtain warrants at all for information voluntarily shared with others; that is to say, voluntarily conveyed information to a third party lacks a reasonable expectation of privacy and thus falls outside the confines of the Fourth Amendment.[31] Telling secrets to frenemies,[32] disclosing financial records to banks,[33] and dialing outgoing (and receiving

[26] *Id.* at 352.
[27] *Id.* at 361 (Harlan, J. concurring).
[28] *Id.* at 352.
[29] Illinois v. Gates, 462 U.S. 213, 236 (1983).
[30] Johnson v. United States, 333 U.S. 10, 14 (1948).
[31] United States v. Miller, 425 U.S. 435, 443 (1976) (noting that "information revealed to a third party and [then] conveyed to Government authorities" is not protected by the Fourth Amendment).
[32] Hoffa v. United States, 385 U.S. 293, 311 (1966).
[33] *Miller*, 425 U.S. at 436.

incoming) telephone numbers[34] are real factual scenarios in which the Supreme Court applied the third-party doctrine.[35]

Accordingly, whether police conduct a search (and therefore need a warrant per the Fourth Amendment) during a criminal investigation becomes a step-by-step query: What did the police do? When did officers acquire a particular piece of information? How did they acquire it? What did they do next? Each "discrete step" of police action forms what has been termed a "sequential approach" to current Fourth Amendment analysis.[36]

Following a sequential methodology to determine when and if a "search" occurs makes sense in the context of traditional police investigations, where police are tracking down tangible evidence like a bloody piece of clothing or the proverbial "smoking gun." Crim Pro students also find this chronological approach helpful when organizing course outlines and answers to essay hypotheticals.

The present combination of powerful police technology and the ubiquity of citizens' cell phones should give pause—and maybe even a hard stop—to the continued applicability of the third-party doctrine, when even a walk to the park creates a "shared" digital trail of cell tower pings and "voluntarily conveyed" images captured on neighborhood security cameras. Taking it a step further, is it clear that the Fourth Amendment search paradigm still protects the people from their government? Strictly from a

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

[35] *But see* Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) (pointing to Orin Kerr as one of numerous scholars who has criticized the third-party doctrine as being "not only wrong, but horribly wrong").

[36] Orin S. Kerr, *An Equilibrium Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 485 (2011) (explaining how the U.S. Supreme Court acknowledges changing technology by adjusting accordingly to allow for continued Fourth Amendment protections.); *see also* United States v. Wright, 2022 U.S. Dist. LEXIS 133312, at *27 (D. N.J. July 27, 2022) (noting one of the "basic truisms of criminal procedure . . . is that the law of search and seizure is highly time-dependent; it depends, not only on what the police knew, but precisely when they knew it").

classroom perspective, how hard should professors push students to consider the constitutional implications of rapidly advancing technology?[37]

Courts have applied the *Katz* doctrine for over fifty years to decide whether Fourth Amendment protections extend to a myriad of different technology. Battery-powered tracking devices (colloquially referred to as "beepers" due to their periodic signals, or "beeps") attached to vehicles driving on public roadways do not require a warrant.[38] If those beepers are brought inside a residential home, then they do require a warrant.[39] Thermal imagers held across the street from homes to detect heat levels inside those homes do require a warrant.[40] GPS transmitters attached to vehicles for twenty-eight continuous days—even when those vehicles drive on public roadways—do require a warrant.[41] Cell phones seized during an arrest cannot be searched without a warrant.[42] Whether the technology at issue was relatively primitive or highly complex, the *Katz* reasonable expectation of privacy test underpins all of these determinations.

The Supreme Court has noted, despite its continued adherence to *Katz*, that analyzing each police act separately may not adequately address how

---

[37] Of course, Crim Pro classes discuss the relationship between the Fourth Amendment and new technology, but now it is imperative to fully integrate this theme throughout the course.

[38] United States v. Knotts, 460 U.S. 276, 285 (1983); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018) (reviewing the "use of a 'beeper' to aid in tracking a vehicle through traffic" in Knotts).

[39] United States v. Karo, 468 U.S. 705, 718 (1984).

[40] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[41] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). In a twist, the majority decision rested on original property and trespass law. However, five justices wrote or joined their own opinions concurring with the result but not with the reasoning; to this day at least two of these powerful concurrences, both utilizing the *Katz* privacy test, are cited more extensively than the majority opinion.

[42] Riley v. California, 572 U.S. 373, 397 (2014) (holding that a cell phone is unlike a regular "container" and therefore is not searchable per the search incident to arrest doctrine).

we the people are affected by the "seismic shifts in digital technology"[43] impacting everyone today. Focusing on the individual steps taken throughout an investigation surely distracts from the Orwellian nature of this "near perfect" police surveillance.[44] It may be unoriginal to fall back on the trope that the law is known to lag behind technology, but the Supreme Court makes an excellent and timely point here.

Our country has more cell phones than people, and we all tend to "quite compulsively" keep our phones within arm's reach—if not actually in hand—all the time.[45] Modern cell phones "generate increasingly vast amounts of increasingly precise CSLI [cell site location information]" making it very simple for police to collect unthinkable amounts of digital data from their signals.[46] Indeed, a cell search can yield more personal, deeply intimate information than could be found after physically rummaging through an entire house.

Police and prosecutors have thrown up a wall of defenses: They have "mechanically" pointed to user agreements—those multi-page, fine print documents we all have to sign in order to purchase phones and set up cell service—as proof of our "voluntary conveyance" of CSLI.[47] They have argued that people "consent" to providing CSLI to their cell phone providers and relatedly, that they "consent" to allow cookies when purchasing apps.[48] They have asserted that CSLI is a "business record" owned by wireless cell carriers.[49]

---

[43] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); *see also* United States v. Tuggle, 4 F.4th 505, 510 (7th Cir. 2021) (noting the "challenge to apply Fourth Amendment protections to accommodate forthcoming technological changes").

[44] *Carpenter*, 138 S. Ct. at 2210.

[45] *See id.* at 2211 ("There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.").

[46] *Id.* at 2212 (comparing cell phone tracking to the "traditional investigative tools" used by police in the past).

[47] *Id.* at 2210.

[48] *See* In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) (rejecting the government's argument that "cell phone users have consented to the government's acquisition of … historical CSLI associated with

But the Supreme Court did not buy any of these legal fictions when government agents tracked a federal defendant's previous movements by collecting and chronicling the CSLI from his cell phone. In *Carpenter v. United States*, a suspect in a series of cell phone store robberies gave up the cell numbers of his co-conspirators to the police, including Mr. Carpenter's cell number.[50] The government obtained a court order, but not a warrant, to compel Mr. Carpenter's cell service provider to furnish months' worth of geo-spatial data points which ultimately placed Mr. Carpenter (or at least, his phone) at the scene of several of the robberies.[51] The Supreme Court found that this type of "tireless and absolute surveillance" required a warrant.[52]

The Court marveled at the unique investigative capabilities of CSLI when it noted that "the retrospective quality of [CSLI] data gives police access to a category of information otherwise unknowable . . . police need not even know in advance whether they want to follow a particular individual, or when."[53]

The heart of the *Carpenter* decision is stated in its holding:

> [W]e decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of

---

their cell phones" and using the government's own argument against it when showing the government's inability to "provide the most recent privacy policies for each telephone service provider listed in the government's application").

[49] Brief for United States at 21, United States v. Elmore, 917 F.3d 1068 (9th Cir. 2019) (in which the prosecution argued that "individuals do not have a reasonable expectation of privacy in business records maintained by their cell phone carriers").

[50] *Carpenter*, 138 S. Ct. at 2212; *see also* Elie Mystal, *Supreme Court Continues Its Modernization Campaign: Requires Warrants for Some Cell Phone Searches*, ABOVE THE LAW (June 22, 2018, 2:15 PM), https://abovethelaw.com/2018/06/supreme-court-continues-its-modernization-campaign-requires-warrants-for-some-cell-phone-searches/ [https://perma.cc/MX9G-V9MD].

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

[52] *Id.* at 2218.

[53] *Id.*

> its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.[54]

Therefore, I'm moving *Carpenter* to the start of Crim Pro. It covers numerous issues arising from the confluence of search and seizure law and police surveillance tech. It articulates concerns about the erosion of personal privacy. It follows *Katz* but offers the possibility of a future paradigm shift. It does not overrule the third-party doctrine, but it does not extend it either. It just might be the case that makes students cry out loud—or at least cry out for more guidance.

Regrettably, there is not much guidance to be found quite yet. Lower court rulings are scant, and of the rulings that have been issued, none are binding—or even particularly persuasive—authority. Two recent court cases garnered headlines but failed to live up to the hype.

United States v. Chatrie involved the use of a "geofence warrant" commanding Google to provide the location data from every cell phone that was near the scene of a bank robbery around the time of that crime.[55] Police then analyzed the location records from all of the cell phones that had entered a 150-meter radius before, during, and after that crime.[56] This process is how police first became aware of the defendant, Mr. Chatrie.[57] Rather than address whether this conduct was equivalent to a "search," the court assumed as much because the police had already obtained the warrant before gathering the data.[58] The court held that the warrant violated the

---

[54] *Id.* at 2223.
[55] Also known as a "reverse location search warrant" discussed *infra*.
[56] United States v. Chatrie, 590 F. Supp. 3d 901, 906 (E.D. Va. 2022).
[57] *Id.*
[58] Jim Garland et al., *Federal Court Expresses Skepticism About Validity of Geofence Warrants but Declines Suppression Remedy* (Mar. 9, 2022), https://www.insideprivacy.com/united-states/litigation/federal-court-expresses-skepticism-about-validity-of-geofence-warrants-but-declines-suppression-remedy/ [https://perma.cc/KMX9-GYHT?type=image] (quoting *Chatrie*, F. Supp. 3d at 929,

reasonable expectations of privacy held by the individuals associated with the cell phones that entered the geofence, but nonetheless upheld the warrant pursuant to the good faith exception to the exclusionary rule.[59]

In *United States v. Tuggle*, police suspected that Mr. Tuggle was selling drugs, but they did not have the probable cause necessary to obtain a warrant.[60] So, police attached multiple cameras to utility poles around Mr. Tuggle's private residence and amassed eighteen months of continuous surveillance footage.[61] The court held that, per *Katz*, this police conduct did not amount to a search, reasoning that there was not a reasonable expectation of privacy in the front yard of a house.[62] Thus, the court sidestepped the more novel legal issue of lengthy pole camera reconnaissance.

Despite their limited precedential value, these cases are still instructive for students. They underscore the reality that as surveillance technology continues to permeate society, the *Katz* test may become increasingly problematic. Alternative schools of thought have been floated to augment or replace both the third-party doctrine as well as *Katz* itself.[63] And while I am more prone to "teach to the Bar" than to engage in esoteric wanderings with a captive student audience, when multiple Supreme Court justices have examined a proposed *Katz*-substitute, I should examine it with my students as well.

---

n.34 ("the Court assumes for the sake of analysis that the Government's collection of data here is a 'search'").

[59] *Id.*

[60] United States v. Tuggle, 4 F.4th 505, 511 (7th Cir. 2021), *cert. denied*, 212 L. Ed. 2d 7, 142 S. Ct. 1107 (2022).

[61] *Id.* at 511.

[62] *Id.*

[63] *See, e.g.*, Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016); *see also* Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARVARD J.L. & TECH. 367 (2019); *see also* Eunice Park, *Objects, Places and Cyber-Spaces Post-Carpenter: Extending The Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J.L. & TECH 1 (2019).

The "mosaic theory" of the Fourth Amendment recognizes that data collected over long periods of time can provide a comprehensive life "mosaic" of one's movements and behavioral patterns.[64] This theory emphasizes the constant monitoring of everyone in society as a primary consideration in any privacy analysis. Even where each isolated police action may not be deemed a search, "a series of acts . . . [may] amount to a search when considered as a group."[65]

Police themselves refer to digital surveillance tech as "patterns of life analyses."[66] In light of law enforcement's exhaustive societal monitoring, analyzing "government conduct as a collective whole rather than in isolated steps"[67] may be better suited to determine the definition of a search and all of the attendant Fourth Amendment implications. At this point the only certainty is the uncertain sustainability of *Katz*.

Law students, for the most part, do not like guessing games. After the anxious questions asked "for exam purposes" there will surely be a few more.[68] For example: Does the extensive use of surveillance technology change what society now objectively believes to be "reasonable"? Can *Katz* still be a viable test when what society accepts as "reasonable" presupposes knowledge of these police tech tools? Does the entire legal premise of

---

[64] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012).

[65] *Id.*

[66] Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget'*, AP NEWS (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef [https://perma.cc/K3NJ-JLA7] (describing Fog Science as an "obscure cellphone tracking tool" to harness the data from 250 million cell phones "to create location analyses known among law enforcement as 'patterns of life'").

[67] Kerr, *supra* note 64, at 311.

[68] Academics have raised similar questions. *See generally* Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter*, 26 BERKELEY J. OF CRIM. L. 71 (2021); Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 1 (2018); Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, UNIV. ILL. L. REV. (forthcoming 2022).

whether a police "search" has violated a "reasonable expectation of privacy" now merit a change? Is the third-party doctrine dead? Should the Supreme Court implement a bright-line rule using the mosaic theory framework? What about a hybrid test that considers both *Katz* and the mosaic theory? Will this be on the final?

II. GEOFENCE WARRANTS ARE THE NEW NORMAL AND YET AGGRESSIVELY DISREGARD THE FOURTH AMENDMENT

The first few Criminal Procedure classes also introduce students to the Fourth Amendment warrant requirement. Law students (like much of the general public) usually know that police must "get a warrant" under certain circumstances but are unaware of what these circumstances entail. These initial classes lay out the rules under which police can lawfully obtain a warrant: only after proving to a judge that they have probable cause to believe that particular things or people will be found in specific places. Case law defines "probable cause" as a "fair probability" that contraband or evidence of a crime will be found in a specified area.[69] The warrant affidavit must be written "particularly describing the place to be searched, and the persons or things to be seized," meaning the probable cause cannot describe a vaguely general place.[70]

Given the high volume and varied content of information that cell phones can store, it comes as no surprise that more and more warrants today are for digital data. What is surprising, however, is the widespread acceptance of geofence warrants by the courts, especially considering that these warrants appear to violate the Fourth Amendment in multiple ways.[71] Geofence

[69] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[70] U.S. CONST. amend. IV (e.g., "Southern California.").
[71] Brief of Amicus Curiae Google LLC at 18, United States v. Chatrie, 590 F.Supp.3d 901 (E.D. Va. 2022) (in which Google indicates that "geofence requests jumped 1,500% from 2017 to 2018, and another 500% from 2018 to 2019. Google now reports that geofence warrants make up more than 25% of all the warrants Google receives in the United States"); *see also*, *Man Pleads Guilty in Case Testing Use of Geofence Warrants*,

warrants (also called "reverse location search" warrants) are literally the opposite of traditional warrants. Geofence warrants allow police to look for unknown potential suspects by accessing data from all cell phones and mobile devices that were near a crime scene.[72] When these warrants first caught the public's attention their significance was downplayed by law enforcement as just another tool to help solve cold cases, and only sought after exhausting all possible investigative leads. Police seem to have dropped such defensive posturing, perhaps because of the lack of expected judicial pushback.

In fact, judges are issuing geofence warrants not because the police have probable cause to believe a specific person has committed a crime, but because the police have probable cause to believe that Google has data in its computer servers that can help them figure out who committed that crime.[73] And rather than a warrant "particularly describing" the persons and things to be seized, geofence warrants describe the latitude and longitude grid coordinates of the geographic area surrounding the crime scene, and a span of time before, during, and after the police believe the crime occurred.[74]

Interpreting "probable cause" and "particularity" in this way is a curious methodology at best. Student responses after seeing "real life" geofence warrant affidavits run the gamut from confusion to anger to apoplectic awe,

---

SEATTLE TIMES (May 10, 2022), https://www.seattletimes.com/nation-world/nation/man-pleads-guilty-in-case-testing-use-of-geofence-warrant [https://perma.cc/69LQ-2FPS].

[72] Brief of Amicus Curiae Google LLC at 15, *Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022) (noting various ways a device may be located by using multiple inputs including "not only information related to the locations of nearby cell sites, but also GPS signals … or signals from nearby Wifi networks or Bluetooth devices.").

[73] Document 54-1 Geofence Warrant Attachment B (Probable Cause Affidavit), *Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022); *see also* Tim Cushing, *Top Court in Massachusetts Says Cell Tower Dumps are Constitutional (But Only with a Solid Warrant*), TECHDIRT (June 10, 2022) https://www.techdirt.com/2022/06/10/top-court-in-massachusetts-says-cell-tower-dumps-are-constitutional-but-only-with-a-solid-warrant/ [https://perma.cc/VAV7-Z42A] (describing the particularity of geofence warrants as merely particular to "the data law enforcement wants access to").

[74] Cushing, *supra* note 73.

which probably explains why police departments across the country try to keep this practice as low key as possible.

As boilerplate affidavits make clear, Google tracks data in many ways.[75] Location technologies already built into today's cell phones include GPS data, CSLI, Wi-Fi signals, and Bluetooth readings.[76] Google stores this detailed metadata from "hundreds of millions of devices" in its Sensorvault.[77] This Sensorvault is where law enforcement serves its geofence warrants and where Google accepts such warrants.[78] Even the Supreme Court has noted that it is "easy, cheap, and efficient"[79] for police to utilize this technology to their advantage. Why would the police go back to old investigative techniques that require so much more manpower?

Police reason that because most everyone carries a cell phone with them, the odds of the alleged perpetrator also carrying a cell phone at the time of the criminal activity are high.[80] Better yet, police can legitimately report

---

[75] *See also* NACDL FOURTH AMENDMENT CENTER, GEOFENCE WARRANT PRIMER (2022), https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf [https://perma.cc/KJW2-T9WK].

[76] *See* iPhone 14, APPLE, https://www.apple.com/iphone-14/specs/ [https://perma.cc/DAD9-SHLC] (listing iPhone "tech specs"); *see also* Josh Lake, *How Your Mobile Phone Tracks You (Even When Switched Off)*, COMPARITECH (Nov. 25, 2020), https://www.comparitech.com/blog/vpn-privacy/stop-mobile-phone-tracking/ [https://perma.cc/M5ZT-9U5B] (detailing the "tangled mess of data collection" that the technology in mobile phones gathers).

[77] Brief of Amicus Curiae Google LLC, *Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022) (in which Google describes its Location History service and how it is stored and disseminated); *see also* Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for The Police*, N.Y. TIMES, (Apr. 13, 2019) https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/GB3H-VC6A].

[78] Brief of Amicus Curiae Google LLC, *supra* note 77, at 901.

[79] Carpenter v. United States, 138 S. Ct. 2206 (2018) (comparing cell phone tracking to the "traditional investigative tools" used by police in the past).

[80] Indeed, the geofence location requested by police in *Chatrie* included not only the bank that was allegedly robbed but also a church and a parking lot because a witness to the bank robbery told police that the suspect held a phone to his face. *See Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022).

that there is a fair probability[81] that Google will be able to identify the cell phone of the person who the police are ultimately seeking, even if the police do not know who that person is at the time of the requested information.

The narrative promoted by Google and police agencies focuses on Google's self-imposed multi-step process for warrants seeking location history information. A three-step protocol narrows the requested data with each round of warrants.[82] The broad production of anonymized information within and surrounding geofence time and space coordinates tapers to anonymized contextual data points and then to specific names, email addresses, and other account subscriber information.[83] Police stress to magistrate judges that analyzing data belonging to innocent bystanders is impossible because the first geofence warrant provides only non-explicit, non-identified number sequences.

To be sure, this argument is simply dressed up propaganda. For one, it glosses over the dragnet-style search technology that is gathering and saving personal information from not only suspects but everyone else too. For another, it is most certainly possible to identify specific people, whether bystanders or criminal suspects, by tracking a cell phone's movements and length of time at each location in conjunction with publicly available information such as property tax records and social media accounts.[84]

---

[81] I.e., probable cause to believe.

[82] NACDL FOURTH AMENDMENT CENTER, *supra* note 75; *see also* Brief of Amicus Curiae Google LLC at 18, *Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022) (describing police geofence requests as searches that are "uniquely broad").

[83] *See* NACDL FOURTH AMENDMENT CENTER, *supra* note 75.

[84] Karl Bode, *'Anonymized Data' is a Gibberish Term, and Rampant Location Data Sales is Still a Problem*, TECHDIRT (Nov. 22, 2021, 6:25 AM), https://www.techdirt.com/2021/11/22/anonymized-data-is-gibberish-term-rampant-location-data-sales-is-still-problem/ [https://perma.cc/G5YJ-H3PA] (quoting EFF technologist Bennett Cyphers explaining, "If you look at a map of where a device spends its time, you can learn a lot: where you sleep at night, where you work, where you eat lunch . . . [B]ecause of that it's extremely simple to associate one of these location traces to a real person"); *see also* Bennett Cyphers, *How The Federal Government Buys Our*

Studies have proven that only four data points are needed to uniquely identify 95% of the people attached to the mobile devices within any given geofence.[85]

The geofence process also usurps the role of the neutral and detached magistrate. Google's entire three-step process is of Google's own making, the result of negotiations between a private company and the police.[86] Even if it is fair to assume that most judges will not be tech-savvy,[87] a private company should not take over the role of the judge in deciding whether the government has met its probable cause burden.

Finally, police justify these geodumps of personal information as necessary to investigate "high profile" and serious and violent felonies.[88]

Cell Phone Location Data, ELEC. FRONTIER FOUND. (June 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data [https://perma.cc/6A2H-GUMU] (noting that "anonymous data" collected by third-party data brokers "may not include explicitly identifying information like names or phone numbers" but that "this does not mean it is 'anonymous'" because customers can still "track devices to specific workplaces, businesses and homes").

[85] Larry Hardesty, *How Hard Is It To 'De-Anonymize' Cell Phone Data?*, MIT NEWS (Mar. 27, 2013), https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data [https://perma.cc/XS8F-GTP6]; *see also* Kim Zetter, *Anonymized Phone Locator Data Not So Anonymous, Researchers Find*, WIRED (Mar. 27, 2013, 4:10 PM), https://www.wired.com/2013/03/anonymous-phone-location-data [https://perma.cc/QUZ3-X4CW] (noting a 2012 study showing cell tower pings from phone location data "produces a GPS fingerprint that can easily be used to identify a user").

[86] Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for The Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/F99A-NSWC] (quoting ACLU surveillance and cybersecurity counsel Jennifer Granick, "We're depending on companies to be the intermediary between people and the government").

[87] This statement may also be true for many law professors.

[88] Linda Lye, *Covert Surveillance in Orange County and Beyond*, ACLU OF S. CAL. (Sept. 20, 2017, 10:00 AM), https://www.aclusocal.org/en/news/government-documents-show-creeping-covert-surveillance-orange-county-and-beyond [https://perma.cc/2CTA-UCJD] (noting that the Anaheim police department justified its surveillance technology as necessary to "apprehend terrorists" even though this tech has been used "for everything from armed robbery to grand theft").

Claims of "national security" interests also tend to appease the public.[89] But in "real life," police are using geofence warrants to investigate rather ordinary criminal activity. And law enforcement should not resort to fear mongering to sway what they must perceive to be an unaccepting public opinion.[90] Our government may subjectively believe it is reasonable to rummage through every house in a neighborhood to solve crime, but is society really ready to accept these investigations as reasonable? If not, why are we allowing police to do so with our electronic information?

Class time will need to be reserved for the anticipated overload of questions: How can geofence warrants be reconciled with the Fourth Amendment? At what exact point in the geofence process does a "search" occur? If one's home is within a police-generated geofence location, can the data from a cell phone inside the house be gathered? How long can the police keep this data and how should they go about destroying it? Just because police can utilize this technology, should they? Is Google the new touchstone of the Fourth Amendment?

---

[89] *See* Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 541 (2019) (discussing law enforcement's common invocation of the "specter of the sophisticated terrorist."); Jason Kelley, *Podcast Episode: What Police Get When They Get Your Phone*, ELEC. FRONTIER FOUND. (Nov. 16, 2021) https://www.eff.org/fa/deeplinks/2021/11/podcast-episode-what-police-get-when-they-get-your-phone [https://perma.cc/MB2R-5PW3] (featuring Executive Director of Upturn Harlan Yu, noting that police use mobile device forensic tools to extract data in felony cases as well as "graffiti, shoplifting, vandalism, traffic crashes, parole violations, petty theft, public intoxication").

[90] City of Indianapolis v. Edmonds, 531 U.S. 32 (2000) ("[T]he gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement may employ to pursue a given purpose.").

III. POLICE ARE BUYING CSLI AND OTHER CONSUMER DATA FROM PRIVATE TECH VENDORS AND THUS BYPASSING THE FOURTH AMENDMENT ALTOGETHER

One more "real life" situation completes the Crim Pro recharge.[91] The facts are a bit disturbing, but the issues are right on point with the Fourth Amendment lessons kicking off this course.[92] Students will have just learned that government action is required to trigger Fourth Amendment protections; the unrelenting proliferation of police surveillance tech has not changed this principle. It has, however, incentivized a private marketplace of location data brokers who sell consumer CSLI to every level of government, no warrant required.[93] To be clear: law enforcement has bought and are still buying our CSLI data, without any judicial approval, from shady companies just looking to turn a profit. There are no coherent rules for an industry engaged in buying and selling billions of dollars' worth of app-generated cell phone location coordinates to the government, including federal immigration agencies, the military, and local police departments.[94] This subversion has been going on for years—it is not a secret, and there is no resolution in sight.[95]

---

[91] For now.

[92] *See* DRESSLER ET AL., *supra* note 1, at 98 (questioning the relevance of the *Katz* concept of privacy in recent years).

[93] Sophie Bushwick, *Yes, Phones Can Reveal if Someone Gets an Abortion*, SCI. AM., (May 13, 2022) https://www.scientificamerican.com/article/yes-phones-can-reveal-if-someone-gets-an-abortion/ [https://perma.cc/9J84-J8PA] (quoting Stanford Internet Observatory research scholar Riana Pfefferkorn, "Law enforcement agencies have used data brokers to do an end run around the Fourth Amendment's warrant requirement. They just buy the information they'd otherwise need a warrant to get").

[94] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (and Why it Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/FNQ3-ULCX] ("The United States doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms . . . designed to target only specific types of data in special (often outdated) circumstances"); Cyphers, *supra* note 84.

[95] *See* David C. Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 407 (2013) (noting the many sources data brokers use to obtain personal

It is true that courts across the country regularly debate what standard of protection, if any, should be afforded to keep electronic data private. But congressional interest in regulating the retention and destruction of electronic data only seems to come in fits and starts. The handful of existing federal statutes—written before most of today's technology was even conceived—are ill-suited to cover current electronic communications issues.[96] Legislation that does get proposed often goes nowhere or takes too long to enact.[97] And the public and political apathy prolongs the gridlock and is, to put it mildly, disheartening.

In contrast, California is one of the rare states with updated and expansive digital privacy laws. California residents and consumers enjoy numerous digital privacy rights that include disclosure of the businesses collecting and selling personal information about the consumer and the ability to limit or opt-out of the sale of such information.[98] In fact, California is the first state in the nation to create an agency exclusively devoted to policing online privacy and, eventually, enforcing data protection rules.[99] Lawmakers expect the new California Privacy Protection Agency (CPPA) to rein in the erratic data business practices of Google and

information); Gennie Gebhart, *Bad Data "For Good": How Data Brokers Try to Hide Behind Academic Research*, ELEC. FRONTIER FOUND. (Aug. 16, 2022), https://www.eff.org/deeplinks/2022/08/bad-data-good-how-data-brokers-try-hide-academic-research [https://perma.cc/CXW8-HYPT] (noting consumers do not meaningfully consent to "the laundry list of data sharing, selling, and analysis that any number of shadowy third parties are conducting in the background").

[96] *E.g.*, Stored Communications Act, 18 U.S.C. § 2701.

[97] Fourth Amendment Is Not For Sale Act, S.1265, 117th Cong. (2021) (introduced by twenty senators on April 21, 2021; a companion bill was introduced in the House on the same day. To date, nothing more has been accomplished.).

[98] CAL. CIV. CODE § 1798.100.10 et. seq. (West 2020); CAL CODE REGS. tit.11, §§ 999.300 et. seq. (2022).

[99] David McCabe, *How California is Building the Nation's First Privacy Police*, N.Y. TIMES (Mar. 15, 2022), https://www.nytimes.com/2022/03/15/technology/california-privacy-agency-ccpa-gdpr.html [https://perma.cc/TY4T-J9XA] (noting that the California Privacy Protection Agency is currently under construction with an annual budget of $10 million and an employment target of over thirty people).

other tech industry giants.[100] To this end, the CPPA originally set an ambitious pace, drafting a flurry of rules on calendar for public commentary, and ultimate adoption set for late 2022.[101] Various delays in implementation have pushed this timeline to 2023.[102]

Yet California's progressive stance has not stopped law enforcement from blatantly and continuously violating state privacy protection laws. For example, warrants authorizing electronic searches must comply with statutory public disclosure and notice rules, but by asking courts to indefinitely seal the warrant affidavits and returns, police have found a workaround to these laws.[103] As another example, police are legally required to report all geofence warrant requests to California's Open Justice database, but simply choose not to do so; this noncompliance was only discovered when Google filed its own transparency report reflecting thousands of geofence warrants that were not mirrored in the law enforcement database.[104] And for yet another example, information collected by automatic license plate readers (ALPR) may only be lawfully shared with other California agencies, but San Diego police gave away the

[100] *Id.*
[101] Aaron J. Burstein et al., *CPRA Rule Revisions Unlikely to be Finalized in 2022*, (Nov. 7, 2022), https://www.adlawaccess.com/2022/11/articles/cpra-rule-revisions-unlikely-to-be-finalized-in-2022/ [https://perma.cc/ZK2J-UNHP].
[102] *Id.*
[103] Aaron Mackey & Dave Maass, *EFF Continues Legal Fight to Release Records Showing How Law Enforcement Uses Cell-Site Simulators*, ELEC. FRONTIER FOUND. (Dec. 17, 2021), https://www.eff.org/deeplinks/2021/12/eff-continues-legal-fight-release-records-showing-how-law-enforcement-uses-cell [https://perma.cc/TKQ7-5BX4].
[104] Maddy Varner & Alfred Ng, *Thousands of Geofence Warrants Appear to be Missing From a California DOJ Transparency Database*, THE MARKUP (Nov. 3, 2021, 8:00 AM), https://themarkup.org/privacy/2021/11/03/thousands-of-geofence-warrants-appear-to-be-missing-from-a-california-doj-transparency-database [https://perma.cc/6R73-5F9U] (comparing Google's 2019 report declaring it was served with 1,537 geofence warrant requests to California's 2019 law enforcement report declaring it requested 168 such warrants from Google).

ALPR data of tens of thousands of Californians to outside agencies for years.[105]

Admittedly, it's a lot to digest. Students risk cognitive overload at this point.[106] They just spent two ninety-minute class segments and at least twice that amount of prep time[107] critically analyzing the government's promise to not intrude into the lives of its people without prior judicial approval. Buying and sharing our private cell phone data seems like the antithesis of Fourth Amendment adherence. And so my students' questions are my own questions, too: Why study the law at all if the law is being broken quite freely and easily by those sworn to uphold it? How can we trust our justice system to be equitable and inclusive if justice system officials are indiscriminately purchasing our personal information? What is a right without a remedy? Where is the outrage?

IV. CONCLUSION

It will take some time to realistically assess the impact of surveillance technology on Fourth Amendment protections. Most people live outside the bubble that is academia and consequently may be less aware of and even

[105] Cody Dulaney, *Police in San Diego County Breaking the Law Sharing Drivers' Data*, INEWSOURCE (Jan. 6, 2022), https://inewsource.org/2022/01/06/police-share-license-plate-data/ source.org/2022/01/06/police-share-license-plate-data/ [https://perma.cc/JL93-E24Y]; *see also* Cody Dulaney, *Escondido, La Mesa Police Refuse to Stop Sharing Drivers' Location Data Across the U.S. Despite Legal Concerns*, CBS8 (Jan. 24, 2022, 12:38 PM), https://www.cbs8.com/article/news/local/inewsource/escondido-la-mesa-police-refuse-stop-sharing-drivers-location-data-across-the-us/509-36711e71-52ba-4c77-a88a-4657582c0faa [https://perma.cc/6FNT-F9MP].

[106] *See* Maj. Steven Szymanski, *Is the Fourth Amendment Really For Sale? The Defense Intelligence Agency's Purchase of Commercially Available Data*, J. NAT'L SEC. L. & POL. (June 9, 2021), https://jnslp.com/2021/06/09/is-the-fourth-amendment-really-for-sale-the-defense-intelligence-agencys-purchase-of-commercially-available-data/ [https://perma.cc/3GJ5-N365] (noting that "the idea of government agencies purchasing and storing location data is unpopular").

[107] STANDARDS & RULES OF PROC. FOR APPROVAL OF LAW SCHOOLS, Standard 310(b)(1) AM. BAR ASS'N (2015) (setting forth the minimum amount of doctrinal class time combined with preparation time out of class to equal one credit hour).

less interested in constitutional doctrine. Law students will need to prepare for the time when they become lawyers and have to reconcile the "real world" of police investigations with the case law they read in school. For now, they must continue to walk on a Constitutional Criminal Procedure path full of twists, turns, and those zigs and zags.