# Video Analytics and Fourth Amendment Vision

Andrew Guthrie Ferguson*

*What does the Fourth Amendment have to say about video analytics running on citywide camera systems?*

*Video analytics (also known as computer vision) involves hardware and software in cameras that turn video surveillance streams into useful data, identifying, categorizing, matching, and alerting police about objects, people, and incidents. Video analytics can identify objects (e.g., hat, backpack, person, car) and track that person or thing back in time and through the streets using video surveillance footage. For police officers conducting virtual patrols or retrospective investigations, video analytics lets police scan thousands of linked cameras for suspicious behavior or a particular suspect, thus drastically enhancing police surveillance power.*

*The Fourth Amendment question is whether this form of police investigation is a "search," violating a reasonable expectation of privacy. Traditional Fourth Amendment doctrine has long allowed video cameras in public under the theory that people have negligible expectations of privacy in public areas. The open question is whether a digital video analytics system that allows for citywide continuous object identification, classification, matching, tracking, sorting, and storing of images changes the constitutional analysis.*

*This Article argues that video analytics presents a different constitutional problem than traditional video surveillance. Properly understood, what is happening behind the scenes with video analytics should alter the reasonable expectation of privacy analysis. This Article builds upon recent Supreme Court cases to develop a theory for when digital surveillance becomes a Fourth Amendment search.*

*The Article also uses video analytics to explore the limits of Fourth Amendment doctrine. Interestingly, the tension in applying the existing Fourth Amendment framework to the puzzle of video analytics reveals several unstated but important assumptions that may need reexamination in*

* Thank you to Professors Kate Weisburd, Itay Ravid, Melanie Reid, Guha Krishnamurthi and the ABA/Criminal Justice Section Workshop for helpful comments on this Article. Thank you to Katrina Geddes, Steven Bellovin, Maneka Sinha, Sharon Bradford Franklin, Clare Garvie, Dan Calacci, Marc Cannellas, Sarah Lageson, Shane Ferro and the rest of the Privacy Law Scholars Conference commentators. Thank you to Professors David Abrams, Chaz Arnett, Valena Beety, Jessica Eaglin, Corinna Barrett Lain, Erin Murphy, Andrea Roth, Meghan Ryan, Maneka Sinha, Christopher Slobogin, and Jenia Turner for thoughtful input at the SMU Tsai Center academic workshop. Thank you to Caitlyn Greene at AUWCL and Mert Karakya at IPVM.

*the digital age. In fact, the rise of video analytics both presents one of the most significant privacy-eroding technologies ever deployed, and at the same time, one of the best opportunities to confront the gaps in existing Fourth Amendment doctrine. Like the innovation behind computer vision itself, digital analytics invites a new way of envisioning the Fourth Amendment.*

## Introduction

In cities across America, Real-Time Crime Centers monitor the streets.[1] Surveillance cameras feed video monitors, sensors alert to unusual activities, automated license plate readers scan passing cars, gunshot detection systems report loud sounds, and community-aided dispatch calls animate a central command center.[2] The fusion of various technologies allows real time response to emergencies and retrospective investigation into past crimes. Real-Time Crime Centers have been promoted as the next evolution of law enforcement and promise a central surveillance hub of police intelligence to monitor big and small cities alike.[3]

1. Zac Larkham, *The Quiet Rise of Real-Time Crime Centers*, WIRED (July 28, 2023, 7:00 AM), https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/ [https://perma.cc/8D4X-5MD8]; *see also Surveillance Compounded: Real-Time Crime Centers in the U.S.*, ATLAS OF SURVEILLANCE, https://atlasofsurveillance.org/real-time-crime-centers [https://perma.cc/3Z8Z-QELL] (mapping cities with real-time crime centers); Jahd Khalil, *Real Time Crime Centers, Which Started in Bigger Cities, Spread Across America*, NPR (Aug. 16, 2023, 5:10 AM), https://www.npr.org/2023/08/16/1194115202/real-time-crime-centers-which-started-in-bigger-cities-spread-across-the-u-s [https://perma.cc/YLN8-ZXY3] (estimating the current number of RTCCs at 135 and growing).

2. Jason Tyre, *How Technology Powers Real Time Crime Centers*, POLICE MAG. (Sept. 27, 2023), https://www.policemag.com/technology/article/15635270/how-technology-powers-real-time-crime-centers [https://perma.cc/W4MV-6K44] ("RTCCs can integrate data from security cameras, gunshot sensors, and many other technologies to help identify threats and guide law enforcement responses in real time."); Keely Quinlan, *Police Real-Time Crime Centers Are Becoming Data Powerhouses*, STATESCOOP (Aug. 24, 2023), https://statescoop.com/real-time-crime-centers-police-privacy/ [https://perma.cc/7Q84-WSBL] ("Crime centers are consolidating information from traffic cameras, drones, gunshot detection sensors and other sources of intelligence into single platforms.").

3. Susan Montoya Bryan, *Leaders Seek to Expand Crime-Fighting Net of Cameras and Sensors Beyond New Mexico's Largest City*, ASSOCIATED PRESS (Dec. 18, 2023, 7:52 PM), https://apnews.com/article/albuquerque-crime-cameras-technology-f63d9e13cbf3321a391f6ce71ed764e6 [https://perma.cc/F48S-R3Z9] ("Video feeds from city intersections and bus stops played out simultaneously on a massive screen that covered one wall as individual stations were outfitted with numerous smaller monitors."); *see also, e.g.*, Calvin Hennick, *Command Centers Turn to Video Surveillance to Improve Response Times*, STATETECH (July 19, 2022), https://statetechmagazine.com/article/2022/07/command-centers-turn-video-surveillance-improve-response-times [https://perma.cc/9STX-UB3V] (outlining how the implementation of the RTCC boosted crime-fighting abilities for law enforcement in Newport News, Virginia); Jim McKay, *Crooks Can't Dodge the Real-Time Crime Center 'Double Click*,' GOV'T TECH (Dec. 7, 2023), https://www.govtech.com/em/crooks-cant-dodge-the-real-time-crime-center-double-click [https://perma.cc/KH59-T6GG] (describing how the new RTCC in Mesa, Arizona has increased the efficiency of the police force); Elena Barrera, *'Nerve Center': Real-Time Crime Center Helps Solves Cases in Hours Instead of Days*, TALLAHASSEE DEMOCRAT (Sept. 16, 2023, 12:47 PM), https://www.tallahassee.com/story/news/local/2023/09/15/law-enforcement-unites-real-time-crime-center-leon-county-tallahassee-tpd-lcso-fsu-shootings/70864256007/ [https://perma.cc/W85H-PYYF] (outlining how the RTCC in Tallahassee assists the police force while they are in the field).

At the core of these centralized surveillance systems is video analytics.[4] Video analytics (also known as computer vision) involves hardware and software in cameras that turn those constant video surveillance streams into useful data, identifying, categorizing, matching, and alerting police about objects, people, and incidents.[5] Powering that video analytics is artificial intelligence (AI) that allows for sophisticated pattern-matching technologies to work through vast quantities of information.[6] An otherwise overwhelming volume of city data becomes searchable when converted into recognizable and sortable objects and fields.[7] In simplified form, video analytics digitizes and thus allows each of the objects on the screen (people, cars, animals, bags, floppy hats, sneakers) to be separated out, categorized, isolated, and tracked across time and place.[8] With the click of a few buttons, police analysts can use computer vision to find all the white vans, red hats, and men carrying umbrellas (or other objects) and track those identified persons or things back

4. Brandon Block, *Federal Aid Is Supercharging Local WA Police Surveillance Tech*, CROSSCUT (July 26, 2023), https://crosscut.com/investigations/2023/07/federal-aid-supercharging-local-wa-police-surveillance-tech [https://perma.cc/8E2P-LEBQ] (discussing the Spokane live map hub and the $150,000 video analytics software that utilizes machine learning to scrub through footage for more efficient policing).

5. JOHN S. HOLLYWOOD, MICHAEL J.D. VERMEER, DULANI WOODS, SEAN E. GOODISON & BRIAN A. JACKSON, USING VIDEO ANALYTICS AND SENSOR FUSION IN LAW ENFORCEMENT, RAND CORP., at 4 (2018) (describing video analytics); Stephen T. Black, *Who Owns Your Data?*, 54 IND. L. REV. 305, 337 (2021) ("Computer vision tries to replicate human pattern recognition and process images or videos in real time."); LAWRENCE J. FENNELLY, EFFECTIVE PHYSICAL SECURITY 122 (5th ed. 2017) ("Video analytics is a technology that processes a digital video signal using a special algorithm to perform a security-related function. There are three common types of video analytics: fixed algorithm analytics, artificial intelligence learning algorithms, and facial recognition systems.").

6. Paul W. Grimm, Maura R. Grossman & Gordon V. Cormack, *Artificial Intelligence as Evidence*, 19 NW. J. TECH. & INTELL. PROP. 9, 14–15 (2021) (explaining the general difference between what computers can generally do now ("narrow" or "weak" AI) and the aspirational goal of "general" or "strong" AI, which is rivaling human performance in a wide range of tasks); *see, e.g.*, *What Is Video Analytics?*, BRIEFCAM, https://www.briefcam.com/technology/video-analytics [https://perma.cc/2WCQ-UHWH] (explaining that Video Analytics is the process of transforming videos into quantifiable data which artificial intelligence can act upon).

7. Jay Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, ACLU, June 2019, at 3, 17–19, https://www.aclu.org/publications/dawn-robot-surveillance [https://perma.cc/96XH-VA53] (describing how the technology "can be used to alert the authorities when something or someone deemed 'suspicious' is detected, or to collect detailed information about video subjects for security or marketing purposes"). For a wonderful description of how machine vision works, see JILL WALKER RETTBERG, MACHINE VISION: HOW ALGORITHMS ARE CHANGING THE WAY WE SEE THE WORLD 6–8 (2023).

8. Luke Stark & Jevan Hutson, *Physiognomic Artificial Intelligence*, 32 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 922, 940 (2022) ("Computer vision systems are grounded in digitalization, or breaking the observable world down into binary code and extrapolating salient features out of the resulting data."); *see also* MAHESHKUMAR H. KOLEKAR, INTELLIGENT VIDEO SURVEILLANCE SYSTEMS: AN ALGORITHMIC APPROACH 75 (2018) ("Object classification detects moving objects in a video sequence and classifies them into categories such as humans, vehicles, birds, clouds, or animals.").

in time across the cameras.[9] In addition, automated prompts can be programmed to identify objects (e.g., a gun or a backpack) or unusual patterns of activity (e.g., movement in an empty park at 2:00 AM).[10] Almost everything in the video streams is being identified and classified into objects or movements, giving police a visual superpower to process more data than ever before.[11]

This Article addresses the rise of video analytics in Real-Time Crime Centers and other centralized policing surveillance systems. As with other policing technologies, a constitutional limit may exist for the wide-scale use of these surveillance systems.[12] This Article addresses how the Fourth Amendment fits video analytics, focusing specifically on video analytics in Real-Time Crime Centers.[13] This constitutional focus is necessary because no federal, state, or local statutes or ordinances regulate the use of Real-Time Crime Centers,[14] leaving rulemaking to local policy and departmental practice.[15] There are also no federal or state laws which regulate video analytics in general, although some jurisdictions have responded to subtypes of video analytics like facial recognition and automated license plate readers

---

9. Erin Tracy, *Not Just Surveillance: Riverbank's New Cameras Recognize When You're Up To No Good*, MODESTO BEE (June 25, 2019, 10:35 AM), https://www.modbee.com/news/local/article231746063.html [https://perma.cc/D7AN-LRJU]. Reporting the comments of the surveillance company's CEO, Tracy notes that

> The cameras can pan, tilt and zoom in from about a mile away . . . . Police in Fremont used the RSUs to identify and arrest a bank robber by zooming in on a tattoo on his forearm as he fled in a vehicle onto a nearby freeway. By entering the license plate into the system, they saw video of him casing the area the day before the robbery.

*Id.*

10. *Id.* ("Riverbank's newest surveillance cameras . . . can detect when someone stops a car and dumps trash along a roadway. They can track a specific vehicle as it goes through town after, say, a bank robbery. And through them, authorities can talk to suspects at the exact time they're doing something illegal.").

11. Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 717 (2017) (explaining how certain tracking technology "allows law enforcement to overlay hours of video and then isolate individuals . . . so monitors can view all applicable targets with hours of time reduced to minutes").

12. This Article focuses on the Fourth Amendment. Other constitutional challenges exist. For example, all video analytics systems capture exculpatory information as well as inculpatory information, yet how the due process requirements of *Brady v. Maryland* fit the technological reality of RTCCs or video analytics has not been addressed. *See* Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180, 206–17 (2020) (discussing *Brady* issues with citywide surveillance systems). In addition, intentional and discriminatory use of cameras in particular areas or targeted against particular people may raise an equal protection challenge.

13. The details of video analytics will be discussed *infra* Part I.

14. *See* Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1160, 1163–64 (2022) (describing the lack of legislative protections for new forms of surveillance technology).

15. Block, *supra* note 4 ("[O]n the local level these technologies often roll out with little oversight, leaving departments to decide for themselves, for example, if they want to use the data to assist with immigration enforcement or share data with states where seeking an abortion is a crime.").

(ALPRs).[16] Without legislative or constitutional checks, new forms of AI-enhanced digital surveillance systems continue to expand.[17]

The Article also uses video analytics to explore the limits of Fourth Amendment analysis in a digital age. Interestingly, the tension in applying the existing Fourth Amendment framework to the puzzle of video analytics reveals several unstated but important doctrinal principles that may need reexamination.[18] Questions about humans in the loop,[19] tools versus systems, time, scope, and scale, and the expectations of privacy in public all become heightened when the Fourth Amendment is forced to confront citywide systems of digital video surveillance.[20] In fact, as I will argue, the rise of video analytics presents both one of the most significant privacy- and liberty-eroding technologies ever deployed, and at the same time, one of the best opportunities to confront the gaps in existing Fourth Amendment doctrine. Like the innovation behind computer vision itself, digital analytics allows a new way of envisioning the Fourth Amendment.

Part I of this Article begins with an exploration of the technical capacities of video analytics in the early age of AI. For clarity, this discussion will focus on video analytics built into citywide Real-Time Crime Centers, although analytics technology can be used on video streams from police body cameras, private residential surveillance cameras, private commercial

16. For example, several smaller jurisdictions have regulated or banned facial recognition. Yet, the broader category of video analytics is not subject to federal or state law. Associated Press, *States Push Back Against Use of Facial Recognition by Police*, U.S. NEWS (May 5, 2021, 1:20 PM), https://www.usnews.com/news/politics/articles/2021-05-05/states-push-back-against-use-of-facial-recognition-by-police [https://perma.cc/P3GA-6LPJ]; Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (April 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/#top62 [https://perma.cc/CNT2-DTHK] ("[S]tate and local regulations lack uniformity throughout the country, and the majority of municipalities do not have specific legal restrictions on government use of facial recognition."). Similar piecemeal restrictions exist for ALPRs. *See Automated License Plate Readers: State Statutes*, NCSL (Feb. 3, 2022), https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes [https://perma.cc/FX74-JZ3Y] (noting that at least 16 states have enacted statutes to address ALPRs).

17. Lee & Chin-Rothmann, *supra* note 16 ("Technological advances have expanded government surveillance in traditionally 'public' places, prompting legal questions over the boundaries between permissible and non-permissible data collection.").

18. *See infra* Part II.

19. Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 VAND. L. REV. 429, 440 (2023) (describing the concept as "an individual who is involved in a single, particular decision made in conjunction with an algorithm").

20. These terms will be discussed *infra*, but questions about whether algorithms will make decisions without humans (humans not in the loop) and the difference digital technology makes in terms of the amount of data that can be collected and utilized are all central to the discussion in Part II.

surveillance cameras, and university and secondary school cameras.[21] Video analytics as a hardware and software tool can be overlayed onto any digital video surveillance system.[22] For law enforcement purposes, video analytics is used in three main ways: (1) observational monitoring (virtual patrols);[23] (2) incident investigation (retrospective searches);[24] and (3) anomaly detection (unusual activity alerts).[25] In practical effect, once deployed, police can monitor the cameras in real time, query the database to review incidents, and respond to algorithmic alerts preprogrammed in the system.[26] Each use case presents different Fourth Amendment issues, but all are central to the everyday functioning of Real-Time Crime Center systems.

Part II explores the Fourth Amendment's confused approach to privacy in public. Two divergent sets of cases exist that govern the question of

---

21. *See, e.g.*, Jennifer A. Kingson, *New AI Tool Instantly Analyzes Police Bodycam Footage*, AXIOS (Jan. 30, 2023), https://www.axios.com/2023/01/30/police-tyre-nichols-bodycam-footage [https://perma.cc/B54L-F2VK] ("A small but growing number of police departments are using a new AI system that analyzes officers' bodycam footage and flags problematic encounters—as well as commendable ones."); Dean Takahashi, *ZeroEyes Uses AI and Security Cameras to Detect Guns in Public and Private Spaces*, VENTUREBEAT (July 31, 2023, 6:30 AM), https://venturebeat.com/ai/zeroeyes-uses-ai-and-security-cameras-to-detect-guns-in-public-and-private-spaces/ [https://perma.cc/52ZT-UQZQ] (discussing several commercial uses of AI-enhanced surveillance); Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch over Public Housing*, WASH. POST (May 16, 2023, 6:03 AM), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/ [https://perma.cc/7FQQ-LBLN] (expressing concern over increased use of AI surveillance in public housing facilities); Matt Mencarini, *Michigan State Expands Surveillance, with an Eye Toward How Artificial Intelligence Can Help*, LANSING STATE JOURNAL (May 12, 2023, 9:43 AM), https://eu.lansingstatejournal.com/story/news/local/2023/05/12/michigan-state-surveillance-cameras-ai-artificial-intelligence-security/70198890007/ [https://perma.cc/5UPN-ELXX] (describing the implementation of an AI-capable surveillance system at Michigan State University).

22. *See What Is Video Analytics?*, *supra* note 6 (explaining that video analytics can be overlaid onto video surveillance networks).

23. Avi Asher-Schapiro, *Privacy or Safety? U.S. Brings 'Surveillance City to the Suburbs'*, REUTERS (May 11, 2023, 4:01 AM), https://www.reuters.com/article/technology/privacy-or-safety-us-brings-surveillance-city-to-the-suburbs-idUSL8N35O0IE/ [https://perma.cc/E543-HJYG] (discussing the reality of video "virtual patrols").

24. Michael Isaac Stein, '*Holy Cow': The Powerful Software Behind the City's Surveillance System*, THE LENS (Dec. 20, 2018), https://thelensnola.org/2018/12/20/holy-cow-the-powerful-software-behind-the-citys-surveillance-system/ [https://perma.cc/82XA-QWFL] (describing the investigative power of video analytics on New Orleans camera systems).

25. *See Paris 2024 Olympics*: *Concern over French Plan for AI Surveillance*, BBC (July 18, 2023), https://www.bbc.com/news/world-europe-66122743 [https://perma.cc/55GX-DPBB] (discussing anomaly bag detection video technologies).

26. *See* McKay, *supra* note 3 ("The system gives police the ability to listen in on a 911 call in real time and immediately get a visual from the nearest camera. From there the technology allows officers to 'track' a subject by double-clicking on cameras that follow the subject's direction, a feature called Citigraf."); Eoin Higgins, *Pre-Crime Policing Is Closer Than You Think, and It's Freaking People Out*, VICE (June 12, 2018, 3:47 PM), https://www.vice.com/en/article/why-does-hartford-have-so-many-cameras-precrime/ [https://perma.cc/V9KB-L566] (describing how some software can compress hours of video into just the relevant minutes, automating a process that could take days for a human to complete).

whether a person has a reasonable expectation of privacy in movements and information they expose to the public. The "traditional canon" of cases arose out of the analog surveillance realities of the 1960s through the 1990s and generally holds that people can expect little privacy in public spaces.[27] More recent cases address long-term digital tracking, leading myself and others to conceptualize a "digital is different" canon that creates tension with the more traditional cases.[28] Part II explores how the two lines of cases conflict, but also interrogates some of the underlying assumptions that need to be reexamined—if not reimagined—in a digital age.

Part III of the Article addresses how the Fourth Amendment intersects with this new form of video surveillance power. As an initial matter, claiming any expectation of privacy from citywide public surveillance might appear counterintuitive.[29] For decades, police observation of activities in public generally has been considered to fall outside of Fourth Amendment protections.[30] Yet, as will be discussed, video analytics is not simply video surveillance, and a proper understanding of how the technology works alters the traditional Fourth Amendment analysis.

Part III offers a two-step argument for why video analytics in citywide camera systems should be considered a search for Fourth Amendment purposes. The first step examines how the traditional "no privacy in public" logic does not fit the technology behind video analytics and thus should not control the constitutional search question. This first step makes the convincing but limited claim that the question is still open for courts under existing Fourth Amendment doctrine, and the answer is certainly not compelled by precedent. The second step goes further, arguing that the Supreme Court's recent cases on digital surveillance compel a finding that AI-assisted video analytics surveillance in Real-Time Crime Centers is a Fourth Amendment search. Specifically, I argue that the Supreme Court's concern with long-term digital tracking through systems of mass surveillance in *Carpenter v. United States*[31] and *United States v. Jones*[32] suggests that current use of Real-Time Crime Center video analytics is a Fourth Amendment search.

Studying video analytics also impacts Fourth Amendment theory because the puzzle of fitting a new technology to an old law reveals gaps that

27. *See infra* subpart II(B) (discussing cases).

28. *See infra* subpart II(C) (discussing cases and scholarship).

29. As will be discussed in subpart II(B), claiming an expectation of privacy in public cuts against existing Supreme Court precedent.

30. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

31. Carpenter v. United States, 138 S. Ct. 2206 (2018).

32. United States v. Jones, 565 U.S. 400 (2012).

need to be addressed. As more centralized citywide surveillance systems develop, the questions of what constitutional limits exist will need to be addressed at the front end of the debate. The hope for this Article is to provide a framework to align computer analytics and Fourth Amendment analysis in a way that makes sense for a future vision of privacy in a digital age.

Two caveats are in order before beginning the technical and constitutional analysis. First, this Article only addresses video analytics within Real-Time Crime Centers, and not Real-Time Crime Centers themselves.[33] This is an admittedly narrow focus, as video analytics is just one of the many surveillance tools embedded in these centralized surveillance systems.[34] The fact that police are centralizing the many different surveillance capabilities into one system of social control is its own separate concern.[35] Second, this Article focuses on the Fourth Amendment constitutional puzzle of the technology.[36] Many of the privacy and power concerns examined here could be remedied by legislative or policy responses.[37] In fact, it would be easier and preferable if lawmakers resolved some of these difficult questions *ex ante* through democratically approved legislation.[38] However, at the current time, there have been few legislative rules placed upon digital command centers. In fact, the systems are growing into a dominant organizing principle of modern policing without

33. This narrowed approach leaves open questions about how the aggregation of different data sets might impact the reasonable expectation of privacy. Real-Time Crime Centers present a significant challenge to theories of police surveillance because they offer a comprehensive, aggregated, and potentially retrospective dataset of personally identifiable information. Video analytics is just one part of the larger problem with centralized, aggregated systems of surveillance.

34. In fact, some companies like Fusus are blurring this line already, offering to integrate video analytics into the collection of different streams of police data. Asher-Schapiro, *supra* note 23 ("[C]ities can also integrate the Fusus platform with a suite of other big-data policing tools. These include automatic license plate readers, the gunshot detection tool shotspotter, and predictive policing, as well as AI-powered surveillance tools that allow police to scan the city for specific cars, or people.").

35. The subject of the constitutional status of Real-Time Crime Centers is beyond the scope of this Article. The aggregation of numerous real-time surveillance systems presents difficult Fourth Amendment issues. While not addressed directly in this Article, the conclusion that video analytics surveillance violates the Fourth Amendment suggests that other types of similar citywide suspicionless surveillance also violate the Fourth Amendment. *See* Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 77–79 (2020) (discussing how citywide networks raise Fourth Amendment issues).

36. U.S. CONST. amend. IV.

37. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 984 (2023) (recognizing the limits of focusing on rights as opposed to other levers to address privacy); *see also* Barry Friedman, Farhang Heydari, Max Isaacs & Katie Kinsey, *Policing Police Tech: A Soft Law Solution*, 37 BERKELEY TECH. L.J. 701, 717–21 (2022) (describing the failures of legislative regulation over new police technology).

38. Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1889–91 (2015); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 495 (2013) (suggesting that such legislative fixes are difficult).

governmental oversight.[39] While a Fourth Amendment framework is an imperfect response to growing police power, the hope of this Article is to provide courts and scholars with a framework for critical analysis.

## I. Video Analytics: The Technology

This Part explores the technology behind video analytics. The first two subparts detail the technical specifics of how video analytics works. The third subpart details how police use video analytics technology in practice. Understood properly, what is happening behind the video scenes has direct impact on the Fourth Amendment analysis of what police can do without a warrant.

### *A. Video Analytics: Defined*

In oversimplified terms, video analytics is a sophisticated form of pattern matching.[40] Computers do not "see" like humans do.[41] Computer vision matches a collection of pixels to previously identified patterns of pixels. A computer "sees" a bicycle not because it knows what a bicycle is but because the algorithm has been trained to recognize a certain configuration of pixels as a bicycle. In other words, the computer searches a dataset of previously labeled and stored images to match the input image.[42]

The process of video analytics is thus composed of two steps: a present-object identification and a retrospective pattern-matching search.[43] Because

39. ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 28–31 (2017) (describing the rise of data-driven policing among the nation's largest police departments).

40. Much of the information about video analytics in this Article comes from IPVM educational materials. IPVM is a research institute that conducts testing, holds trainings, and publishes information about physical security technology including video surveillance systems. IPVM offers courses and training materials to learn about the basics of video analytics. *See The Authority on Physical Security*, IPVM, https://ipvm.com/about [https://perma.cc/V7XK-TPY5] (showcasing the IPVM "about" page). IPVM Team, *Video Analytics Fundamentals Guide* (Mar. 4, 2021, 10:00 AM), https://ipvm.com/reports/analytics-fundamentals [https://perma.cc/4SKS-U9KK] ("Video analytics apply algorithms or filters to images and video to find patterns or details in the pixels that represent an object (e.g. Person, Face, Vehicle), features (e.g. a nose, a mask, a truck), and/or behaviors (e.g. loitering, unusual movement, fighting).").

41. IPVM Team, *supra* note 40 ("[C]omputers do not 'see' images as people do. When a computer looks at a digitally encoded image, it is a collection of pixels.").

42. JODY BOOTH, WERNER METZ, ANAHIT TARKHANYAN & SUNIL CHERUVU, DEMYSTIFYING INTELLIGENT MULTIMODE SECURITY SYSTEMS: AN EDGE-TO-CLOUD CYBERSECURITY SOLUTIONS GUIDE 66 (2023) ("Traditional Computer Vision (CV) consists of a developer selecting and connecting computational filters based on linear algebra with the goal of extracting key features of a scene, then correlating the key features with an object(s) so the system can recognize the object(s).").

43. The foregoing discussion focuses on video analytics in 2024, recognizing the long history of machine learning and video. *See* RETTBERG, *supra* note 7, at 5 (2023) (recognizing that "[m]achine learning was first used in image recognition" in 1957).

video analytics systems are so efficient, both parts appear to happen instantaneously, but both present identification and past matching must happen for the system to work.[44] As will be discussed, the level of sophistication in the types of video analytics varies widely, as do the capabilities to identify objects, features, or behaviors. Yet, the fundamental underlying process is the same—collected data must be searched and matched to "see" an identified object.[45]

As might be evident, companies building video analytics systems for police must design the process from the front end, first choosing video technologies that allow identification (seeing pixels that represent the bicycle in front of the camera), but also deciding which datasets to use to teach the computer about what a bicycle looks like.[46] Choosing poorly on either side of the design process can create errors in identification.[47] For example, if the bicycle training dataset had included no motorcycles or scooters to differentiate from bicycles, the computer vision might err in confusing the three types of similar two-wheeled objects. Or if the dataset was trained on bikes from the 1880s (like the Penny Farthing with a big wheel up front), the match might miss modern bicycles.

The most important point for Fourth Amendment analysis is to recognize that video analytics is itself an ongoing, active, two-part search process and not a passive, singular observation. It is not the same as a human police officer watching the video screen. While the speed makes the digital object identification look instantaneous, the work has been done on the back end to allow for pattern matching in real time.

---

44. IPVM, 2023 VIDEO ANALYTICS 62 ("Specialized deep learning algorithms are trained for detecting a single object category (e.g. faces, guns, license plates). This allows them to classify target objects in less than 100 milliseconds, which is critical in certain applications, like facial recognition.").

45. In 2019, the ACLU released a comprehensive report on the dangers of video analytics. Stanley, *supra* note 7, at 3–9. In addition, with next generation AI, video analytics will be able to do context-aware searches that will be driven and generated by the AI itself. *See* Zhengye Yang & Richard J. Radke, *Context-Aware Video Anomaly Detection in Long-Term Datasets*, 2024 IEEE/CVF CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION 4002, 4002 (2024), https://arxiv.org/pdf/2404.07887 [https://perma.cc/S659-NLKV] (proposing context-aware video analytics to enhance searches).

46. Adam Zewe, *Can Machine-Learning Models Overcome Biased Datasets?*, MIT NEWS, (Feb. 21, 2022), https://news.mit.edu/2022/machine-learning-biased-data-0221 [https://perma.cc/6KSH-6XYH] ("If the datasets used to train machine-learning models contain biased data, it is likely the system could exhibit that same bias when it makes decisions in practice.").

47. BOOTH ET AL., *supra* note 42, at 73 ("Training a neural network is subject to the classic computer program GIGO, Garbage In, Garbage Out. Poor data labeling, poor quantity of data and poor definition of output classes will yield poor results.").

### *B. Video Analytics: A Primer*

Video analytics is a complicated topic to explain in a non-technical manner. This subpart seeks to simplify the process in a way most relevant to the legal issues discussed later in this Article.

Picture an image of a dark wooden door against a white background. The door is rectangular with a silver handle. The two-dimensional image can be broken down into pixels with shadings representing the outline of the wood. The pixels are shaded in colors along a continuum of gray, with the darkest gray representing the door and the lighter colors representing the shadings of the white background.[48] A computer vision system will identify the contours of the door by the contrast between light and dark pixels.[49] The greater the contrast, the more likely it represents an edge.[50] The computer vision will see the outline of the door as a series of light and dark contrasts and find the rectangular edges accordingly.[51] To then find a match of the object, the algorithm will search for similar edges and contrasts in the dataset it was trained on to recognize objects we know as doors.[52] If we were talking about a brightly colored door, the system would break down the pixels into colors and, using the contrasts, identify basic colors.[53]

Depending on the sophistication of the system, video analytics could be trained to identify doors by feeding the computer algorithm millions of images of different kinds of doors.[54] These images of doors will be labeled "door"[55] and the algorithm will be able to match a door by matching the edges of the pixels.[56] Using the language of AI, this process of taking labeled

48. IPVM Team, *supra* note 40.

49. *Id.*

50. *Id.*

51. *Id.*

52. *See* BOOTH ET AL., *supra* note 42, at 74 ("Classification is identifying the objects detected in a frame. Is it a car, a person, etc.? A classification may have multiple attributes (e.g., car—blue, sedan, Audi), and a frame may give rise to 0, 1, 2, or many classification tasks.").

53. IPVM, *supra* note 44, at 101 ("Color classifying algorithms take the pixel values of the detected objects and output a single color."); *see* Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 695 (2018) ("All digital images are made up of pixels, which are just tiny points of color situated in a two-dimensional array. Each pixel is a composite of three component colors, red, green, and blue, each of which is assigned a value from 0 to 255.").

54. IPVM Team, *supra* note 40; KOLEKAR, *supra* note 8, at 75 ("Object classification detects moving objects in a video sequence and classifies them into categories such as humans, vehicles, birds, clouds, or animals.").

55. This labeling process can be done by humans who are the labor behind many AI systems. Niamh Rowe, *Millions of Workers Are Training AI Models for Pennies*, WIRED (Oct. 16, 2023, 2:00 AM), https://www.wired.com/story/millions-of-workers-are-training-ai-models-for-pennies/ [https://perma.cc/3BV2-CXB6].

56. IPVM, *supra* note 44, at 112 ("Most video surveillance machine and deep learning analytic training is supervised, meaning the training images and video are labeled, and the computer decides what details/values will be used to detect the objects."); BOOTH ET AL., *supra* note 42, at 66 (noting

images and training them is called "supervised learning."[57] More sophisticated AI models might rely on unsupervised learning, which means the computer teaches itself how to identify doors by scanning large datasets of images which include doors and things that are not doors.[58] Because the objects are not labeled, mistakes can occur (for example, the system might train itself to identify dark rectangles and not doors), but usually the system learns well enough to work, and humans laboring to correct the system are also a significant part of the labeling process.[59] Unsupervised learning is cheaper in terms of human effort than supervised learning because it avoids the need to label millions of objects for training sets.[60] Relatedly, if the only information you need is whether the door is opened or closed, a heuristic filter can be added that can show if there was movement of the pixels that corresponded to a rectangular shape opening or closing.[61] For a fixed security camera in a warehouse, the question of the door being opened or closed may be the only thing that matters (not the kind or color of the door). In addition, based on the success of large language models (e.g., ChatGPT, Llama2), innovators have begun creating similar models for object recognition using visual interference transformers.[62] While still in development, these new techniques have proven quite effective at identifying images as particular objects.[63]

---

that "[t]he key feature of traditional CV methodology is that the developer selects which filters to use and, hence, which features will be used to identify an object," which is successful when "the object is well defined and the scene is well understood," but noting that predicting what identifies a given object becomes more difficult as the number of objects or complexity of the scene increases).

57. IPVM Team, *supra* note 40 ("Supervised means the training images are labeled, and the computer decides what details/values will be used to detect the objects. Properly labeled images are critical for machine learning to detect the correct objects.").

58. IPVM Team, *supra* note 40 ("In unsupervised learning, the images are not labeled, and the computer decides how to group the objects.").

59. *See* Josh Dzieza, *AI Is a Lot of Work*, THE VERGE (June 20, 2023, 7:05 AM), https://www.theverge.com/features/23764584/ai-artificial-intelligence-data-notation-labor-scale-surge-remotasks-openai-chatbots [https://perma.cc/GX72-9CQN] (exposing the human side behind AI labeling and the exploitation and drudgery behind object recognition tasks).

60. Of course, the energy costs of training AI models is very high. *See* Kylie Foy, *New Tools Are Available to Help Reduce the Energy that AI Models Devour*, MIT NEWS (Oct. 5, 2023), https://news.mit.edu/2023/new-tools-available-reduce-energy-that-ai-models-devour-1005 [https://perma.cc/TBX4-97HD] (reporting that the energy required to train Chat-GPT's predecessor model was approximately what 1,450 average U.S. households would use in a month).

61. *See* IPVM Team, *supra* note 40 ("A more advanced stage of heuristic analytics is factoring object color variation or height to width ratio to determine what type of object is in motion (e.g. person or vehicle)."); *see also* KOLEKAR, *supra* note 8, at 75–76 (describing the differences between shape-based classification and movement-based classification).

62. Mert Karakaya, *The Future of Video Analytics—CNNs vs. VITs (Visual Inference Transformers*), IPVM REPORTS (Jan. 5, 2024, 9:00 AM), https://ipvm.com/reports/vit-tutorial [https://perma.cc/V84G-S4AH].

63. *Id.*

No matter the method of analytics, the same basic process occurs. A system matches a present image to a dataset of stored images to make an identification.[64] And even with the most sophisticated of deep learning data sets, the training process happens before the video camera is deployed in the field.[65] The magic of video analytics object-recognition only happens because of the intense and expensive labor involved in teaching the machine to recognize the object. Like many things, what looks like magic really is the product of hard work and effort before the moment of reveal.

Again, the key to the accurate identification of an object is the labeling data the system gets trained on.[66] If the goal is to identify guns, then allowing the dataset to include tens of thousands or millions of photographs of guns will make it more likely that the camera will make an accurate match.[67] Finding a dataset of accurately identified guns is critical to accurate pattern matches. Common datasets exist that allow for object recognition training.[68] Well-known datasets like COCO, ImageNet, or Pascal2 offer centralized training sets of all sorts of common images available to purchase.[69] With the rise of machine-learning models, more options exist to train pattern-matching models on large datasets. As mentioned, new generative AI training systems are currently in development.[70] Of course, concerns exist about having sufficient diversity and representative images in a dataset. For example, early facial recognition systems were trained on datasets of mostly white men, creating identification errors when applied to the task of matching Black and

64. There are two main ways machine learning works. You can have a system that identifies features then edges, or a system that identifies edges then features. IPVM Team, *supra* note 40 ("Haar and HOG-based machine learning analytics are similar in that they are human-defined filters but use opposite strategies to detect objects. Haar finds features, then edges. HOG finds edges and then features."). The latter tends to be more accurate. IPVM Team, *supra* note 40 ("HOG can be more accurate than Haar at some tasks, and less prone to errors due to lighting and angles compared to Haar.").

65. IPVM Team, *supra* note 40 ("A common misunderstanding is that deep learning/AI analytics continue to "learn" after installation . . . . However, for most analytics, all learning happens before the analytic is deployed, and uses the factory-trained model, which does not change over time based on activity or objects detected in the field of view.").

66. IPVM Team, *supra* note 40 ("Datasets are used to train deep learning analytics on how to detect or recognize persons, vehicles, behaviors, faces, or any object/action.").

67. *Id.* ("Datasets are typically composed of thousands to millions of labeled images or videos.").

68. Kent Gauen, Ryan Dailey, John Laiman, Yuxiang Zi, Nirmal Asokan, Yung-Hsiang Lu, George K. Thiruvathukal, Mei-Ling Shyu & Shu-Ching Chen, *Comparison of Visual Datasets for Machine Learning*, 2017 PROCEEDINGS OF IEEE CONFERENCE ON INFORMATION REUSE AND INTEGRATION 346, 347–48 (describing various datasets).

69. *Id.*

70. *See* KOLEKAR, *supra* note 8, at 81–86 (providing a technical description of how convolutional neural networks (CNN) work for object recognition).

Brown women (or really anyone who did not fit the training data).[71] Similarly, even labeling men, women, and children becomes fraught with choices that can distort the dataset; non-binary or non-conforming people might be excluded, and labeling age or gender identification can create unnecessary inconsistencies and inaccuracies.[72]

Doors, of course, are simple, static things. Now picture that the dark wooden door is connected to a house in the background of a busy city street. Every object in the digital video frame can be identified as the object we know it as through the same pixel matching. Parked cars, trucks, vans, houses, people, mailboxes, bicycles, animals, and street signs can all be identified by their pixel edges and identified through pattern matching. Now speed up the frame into a moving video and each object can be identified through the same process. This is the task for engineers designing video analytics systems. A cityscape involves numerous predictable and unpredictable objects and activities.

The real world thus adds a degree of difficulty to pattern matching because the images in the frames are moving and have different lighting conditions and angles.[73] A moving bicycle might look different than a static image, making pattern recognition more difficult.[74] Training algorithms on

71. Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7, 2019, 7:00 AM), https://time.com/5520558/artificial-intelligence-racial-gender-bias/ [https://perma.cc/VZ2K-4NCG]; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77, 86 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/Z2XX-GSB3].

72. As some commentators observed with the BriefCam software,

> BriefCam sorts people and objects into specific categories to make them easier for the system to search for. BriefCam breaks people into the three categories of 'man,' 'woman,' and 'child.' Scientific studies show that this type of categorization can misidentify gender nonconforming, nonbinary, trans, and disabled people whose bodies may not conform to the rigid criteria the software looks for when sorting people.

Dave Maass & Matthew Guariglia, *Video Analytics User Manuals Are a Guide to Dystopia*, EFF (Nov. 19, 2020), https://www.eff.org/deeplinks/2020/11/video-analytics-user-manuals-are-guide-dystopia [https://perma.cc/776Q-EEKT]; *see also* Timnit Gebru & Remi Denton, *Beyond Fairness in Computer Vision: A Holistic Approach to Mitigating Harms and Fostering Community-Rooted Computer Vision Research*, 16 FOUNDS. & TRENDS IN COMPUT. GRAPHICS & VISION 215, 229 (2024) ("Attempting to infer or classify identity characteristics can cause harm by denying individuals an opportunity to self-identify. This harm is particularly salient in the context of gender classification systems that systematically misgender trans and non-binary individuals.") (internal citations omitted).

73. IPVM Team, *supra* note 40 ("While many datasets are created with non-surveillance images (e.g. press photos, mugshots, passport/ID images), it is important to train surveillance analytics with surveillance video. Surveillance cameras typically have challenging angles and lighting.").

74. *See* YOOYOUNG LEE, JONATHAN FISCUS, ANDREW DELGADO, LUKAS DIDUCH, ELIOT GODARD, BAPTISTE CHOCOT, JESSE ZHANG, JIM GOLDEN, AFZAL GODIL & DIANE RIDGEWAY, ACTEV 2021 SEQUESTERED DATA LEADERBOARD (SDL) EVALUATION PLAN 4–5, 9–10 (2021), https://actev.nist.gov/pub/Phase3_ActEV_2021_SDL_EvaluationPlan_20210803.pdf [https://perma.cc/F6LC-SHEQ] (discussing pattern recognition testing with dynamic known activities).

datasets of video surveillance with the appropriate labeled object is important for accuracy. In addition, the object (or objects) must be separated out from the background. If each video is broken up into frames, each frame must be further broken down into objects (and background, lighting, and other obstructions). In a cityscape, for example, many different moving objects must be separated out from the background street and buildings. The resulting effect is digitization of each object in recognizable and matchable pixels, located in time and space in a city, and capturing it all in the video screen.

In addition, specialized algorithms for automated license plate readers (ALPRs) and facial recognition provide different challenges. Automated license plate readers are a form of computer vision that turns license plates into recognizable, and thus identifiable, numbers and letters which can be connected to other databases linked to a list of automobile owners.[75] More traditional optical character recognition (OCR) algorithms take characters as inputs and match the edges to identify the letters or numbers.[76] For example, the edges that create the recognizable numbers 1, 2, 3, and 4 can be easily recognized by a system trained to match similar numbers in a dataset. More advanced systems now use machine learning in addition to OCR.[77] The result is a system that can identify a license plate as it passes by the camera and then link it to an identifiable owner from an existing police database.

Facial recognition follows a similar pattern of breaking down facial features into the different component parts (measurements between eyes, nose, mouth, etc.).[78] Once digitized, the different points can be matched to identify similar features and thus identify people.[79] "Traditionally, facial recognition technology has been 'feature-based,' which utilizes identifying measures like one's eyes, nose, and mouth and the distances between these

75. *See* RETTBERG, *supra* note 7, at 83–84 (2023) (discussing the use of ALPRs); Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 609 (2024) (discussing the rise of automation in ALPR technology).

76. IPVM, *supra* note 44, at 139 ("For example 'A' is created with one angled line from left to right, one angled line from right to left, and a horizontal line in the middle. By finding the edges of the character, OCR determines it is an 'A'.").

77. IPVM, *supra* note 44, at 138 ("While [license plate recognition technology] used Optical Character Recognition (OCR) for decades, deep learning-based approaches have grown. Today, a hybrid approach of Machine and Deep Learning plus OCR is common.").

78. CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 9 (2016), https://www.perpetuallineup.org/ [https://perma.cc/S48P-PL53]; Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, INTERCEPT (Jan. 27, 2020, 11:53 AM), https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks [https://perma.cc/TC3J-5SL5] ("Video analytics systems can analyze and search across real-time streams or recorded footage. They can also isolate individuals or objects as they traverse a smart camera network.").

79. Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 3:19 AM), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/Q5H7-SJFA].

features, or 'appearance-based,' which attempts to match the whole face image. In recent years, other forms of face identification have emerged that look at skin textures, shadows, three-dimensional models, or some combination of all of these types."[80] Once faces are turned into a digital faceprint (like a digital fingerprint), they can be matched to a database of stored digital faceprints.[81] Algorithms match the commonality of the probe photo to the database of photos and, as an output, produce a selection of close matches.[82] With video surveillance, facial recognition is more complicated (and less reliable) because issues such as lighting, angle, and limited video quality can interfere with matching.[83] Several false arrests have occurred using facial recognition.[84] The result has been that video analytics companies have relied on more powerful neural networks to try to improve on accuracy for facial recognition.[85]

Other use cases for video analytics involve bag detection (e.g., backpacks, suitcases), unusual movement detection, and anomaly detection.[86] In these situations, the object recognition is trained to recognize an out-of-place suspicious bag (suggesting the possibility of a bomb) or

80. Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1110–11 (2021) (citing Jagdish Chandra Joshi & K.K. Gupta, *Face Recognition Technology: A Review*, 8 IUP J. TELECOMMS. 53, 54 (2016)); Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 J. MECHATRONICS & ROBOTICS 237, 240–41 (2019); Mary Grace Galterio, Simi Angelic Shavit & Thaier Hayajneh, *A Review of Facial Biometrics Security for Smart Devices*, 7 MDPI COMPUTS. 37, at 3 (2018).

81. JOY BUOLAMWINI, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & ERIK LEARNED-MILLER, FACIAL RECOGNITION TECHNOLOGIES: A PRIMER 8–10 (2020), https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf [https://perma.cc/X8CH-JAV3].

82. *Id.*

83. IPVM, *supra* note 44, at 82 ("Another significant problem for face detection, because of the high detail required, is low or uneven lighting. While a person may be clearly visible, low light video can obscure the face with blur, noise, and artifacts[.]").

84. *E.g.*, Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020, 8:00 AM), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/3XCD-YTZK].

85. Industry reports acknowledge this transition:

> The architectures used for video surveillance face recognition have evolved, from primarily using Haar and HOG-based machine learning . . . to current deep learning convolution neural networks (CNNs). CNN architectures offer higher accuracy through the critical process of convolution. CNNs decrease the amount of data processed by breaking the image down into small sections and summarizing that section to create a smaller image that keeps the relevant information. Small, overlapping sections of the image are run through a "kernel/filter" which converts the image into a single piece of the new smaller image, which is called convolution.

IPVM, *supra* note 44, at 127.

86. Olivia J. Greer, Note, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589, 596 (2012) ("The term 'real-time video analytics' refers to a programmable network, which can be built to recognize and flag—in real-time—scenarios such as abandoned packages in the subway.").

movement in crowds that is unusual (perhaps someone entering via an exit) or some unexpected movement (perhaps a bright light in a location that would ordinarily be dark).[87] The programming of such alerts involves programming an alert system to recognize a pattern that does not fit the expected scene.[88]

Finally, video analytics can be used for behavior identification, such as when particular movements are identified to correspond to particular preprogrammed patterns of activity.[89] For example, video analytics has been trained to recognize an altercation or a robbery based on training of videos of fights or convenience store robberies.[90] While more prone to error because of the complexity of matching behaviors (as the difference between a physical assault and a loving bear hug is understood in context), the use for public safety management is evident.

The above list is not exhaustive, but for video analytics applied to police surveillance systems, the categories of object recognition tend to focus on people, vehicles, clothing, bags, license plates, weapons, and other identifying facial or body features.[91] The next subpart explores how object recognition surveillance applies in the real world.

### *C. Law Enforcement Use of Video Analytics*

The foregoing explanation of the technology behind video analytics becomes manifest in a Real-Time Crime Center populated by active-duty

87. *See, e.g.*, Mohammad Ibrahim Sarker, Cristina Losada-Gutiérrez, Marta Marrón-Romera, David Fuentes-Jiménez & Sara Luengo-Sánchez, *Semi-Supervised Anomaly Detection in Video Surveillance Scenes in the Wild*, SENSORS, June 9, 2021, at 3993, 2, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8230050/ [https://perma.cc/DT9A-MUR7] ("In the context of automating anomaly identification from surveillance videos, computer vision algorithms can be employed to sense and notify the abnormal events along with the time frame within which these have occurred.").

88. Kwet, *supra* note 78.

89. IPVM, *supra* note 44, at 110 (describing "human defined rules based on pose estimation, object detection, and other data" as the most common method for building behavior recognition, with "[d]evelopers defin[ing] what activities of interest are . . . (e.g. a person moving quickly and colliding with another person) or a gun detected in a hand (as opposed to a pocket or holster), and when that activity happens an alert is generated").

90. Some companies advertise the ability for their video analytics to identify violence. *See, e.g.*, *Meet Oddity AI*, https://oddity.ai/ [https://perma.cc/78VD-TBUM].

91. IPVM, *supra* note 44, at 90 ("Machine and Deep Learning algorithms are trained for detecting many different types of objects in video surveillance. While persons, vehicles, and faces are the most common, they also detect and classify advanced objects, most commonly in video surveillance: Guns, Bags, Masks, Color of Objects"); *see also id.* at 86–87 ("Knowing what type of vehicle (e.g. car, truck, bus) was detected is valuable information for investigations, and many AI-based vehicle detection analytics include this[.]").

police officers. In Hartford, Connecticut;[92] Chicago, Illinois;[93] and Savannah, Georgia,[94] police officers sit watching video screens. The screens have video analytics like BriefCam[95] (or the equivalent) technology running behind the scenes, able to sort, search, and identify objects.[96] Some cities, like Chicago, have over 32,000 linked cameras offering police access to many parts of the city.[97] Some companies, like Fusus, envision linking tens of thousands of public and private cameras together in a single Real-Time Crime Center.[98] Other cities have less expansive coverage, choosing to focus on downtown

92. Higgins, *supra* note 26; Zeus Kerravala, *Fact or Fallacy: Video Cameras Are More Than Just Another Set of Eyes*, STATETECH MAG. (July 25, 2022), https://statetechmagazine.com/article/2022/07/fact-or-fallacy-video-cameras-are-more-just-another-set-eyes [https://perma.cc/2NDM-T3DL] ("[I]n Hartford, Conn., first responders use surveillance cameras alongside a technology that checks for gunfire and provides the police with a 24/7 visual of what's happening on city streets. Hartford's command center receives real-time views of the activity, which is analyzed together with data feeds from the system.").

93. Tod Newcombe, *How Tech Helped Chicago Police Solve the Jussie Smollett Case*, GOV'T TECH (Feb. 25, 2019), https://www.govtech.com/analytics/how-tech-helped-chicago-police-solve-the-jussie-smollett-case.html [https://perma.cc/2Z6W-2X5C].

94. Jake Shore, *What to Know: New Savannah Police Technology Can ID Suspects by Clothes, License Plates*, GA. PUB. BROAD. (Oct. 27, 2022, 9:47 AM), https://www.gpb.org/news/2022/10/27/what-know-new-savannah-police-technology-can-id-suspects-by-clothes-license-plates [https://perma.cc/U2LW-ZEM5] ("[BriefCam's] video analytics program is employed by several police departments in cities across the country, including Hartford, C.T., Beverly Hills, C.A., Chicago, Detroit and New Orleans. Airports and "smart cities" are also listed as BriefCam customers.").

95. *What Is Video Analytics?*, *supra* note 6; Caroline Haskins, *Many Police Departments Have Software that Can Identify People in Crowds*, BUZZFEED (June 12, 2020, 11:52 AM), https://www.buzzfeednews.com/article/carolinehaskins1/police-software-briefcam [https://perma.cc/EUT8-4UHS] ("Authorities in Chicago; Boston; Detroit; Denver; Doral, Florida; Hartford, Connecticut; and Santa Fe County, New Mexico have also used [BriefCam].").

96. *What Is Video Analytics?*, *supra* note 6.

97. Tammy Webber, *Chicago's Vast Camera Network Helped Smollett Investigation*, ASSOCIATED PRESS (Feb. 22, 2019, 7:58 AM), https://apnews.com/article/ca0fabcc072d4fc4881237772ef25176 [https://perma.cc/Z5PA-HEQX] (describing 32,000 cameras); Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html [https://perma.cc/7VGZ-TLRC].

98. Joseph Cox, *Is Your Local Police Department Using Fusus AI Enabled Cameras? Find Out Here*, 404 MEDIA (Jan. 16, 2024, 8:58 AM), https://www.404media.co/fusus-ai-cameras-map-local-police/ [https://perma.cc/59UR-6YNC] ("More than a hundred local police departments, sheriff's offices, and cities have set up an AI-powered camera system, with nearly 200,000 connected cameras belonging to residents and businesses around the country able to provide 'direct access' to law enforcement, according to a 404 Media analysis of a set of scraped data."). In 2024, Fusus was bought by Axon, a large platform provider of body cameras and digital storage. Jordan Pearson, *Bodycam Maker Axon Is on a Mission to Surveil America with AI*, VICE (Feb. 1, 2024, 4:13 PM), https://www.vice.com/en/article/axon-acquires-fusus-ai-surveillance-retail-healthcare/ [https://perma.cc/D4TK-PFSR] ("Axon acquired Fusus for an undisclosed sum . . . . Fusus operates what it calls 'real time crime centers (RTCC)' which allow police and other public agencies to analyze a wide array of video sources at a single point and apply AI that detects objects and people.").

areas, "high crime areas," or other places with cameras installed.[99] The technology now exists to link private security cameras and city security cameras and law enforcement cameras, providing police a live feed through this growing network.[100] The reality of video analytics is that it can simply be run on top of this network of digital cameras providing the ability to track and trace objects through the camera system or any camera linked to the system. The more cameras that become linked, the broader the reach of the police surveillance system.

It is important to remember that the police have several different options about how to use the video feeds in Real-Time Crime Centers: (1) monitoring; (2) investigation; and (3) anomaly detection. As will be discussed, the existing camera systems can operate with or without video analytics enabled. The difference now is the ability to convert those same video streams into identifiable objects and do something new with the data.

*1. Monitoring Through Virtual Patrols*.—Real-Time Crime Centers allow police to monitor video streams like their own virtual patrol.[101] Police officers can do this in one of two ways. First, human police officers can simply watch the live feeds. Like watching live television, police can conduct "virtual patrols" that allow them to skim across numerous streets in real time, camera to camera.[102] Maybe they see something suspicious and watch the events unfold, or maybe they direct a camera that corresponds to a reported crime or 911 call.[103] Live monitoring does not require any use of video analytics running behind the scenes (although it might use it anyway). Police—as human observers—can just watch the camera feeds and then send in human police officers to investigate.

---

99. Richard Taliaferro, *Police Unlock AI's Potential to Monitor, Surveil and Solve Crimes*, WALL ST. J. VIDEO (May 30, 2019, 10:42), https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517-AE31BE3C5E7E.html [https://perma.cc/HX8A-ZJ5J]; *see* Larkham, *supra* note 1 (discussing the rise of RTCC cameras).

100. The numbers of cameras are high and growing. For example, Atlanta has over 24,000 cameras, Philadelphia has 28,000, San Francisco has 14,000, and even Denver has 12,000. *See* Jurgita Lapienytė, *This Is the Most Heavily Surveilled City in the US: 50 CCTV Cameras per 1000 Citizens*, CYBERNEWS (Sept. 28, 2021, 2:14 PM), https://cybernews.com/editorial/this-is-the-most-heavily-surveilled-city-in-the-us-50-cctv-cameras-per-1000-citizens/ [https://perma.cc/A4YT-AP8D].

101. Asher-Schapiro, *supra* note 23 ("[A]ll newly constructed or remodeled commercial and industrial properties in the city were required by the police to register cameras . . . and allow police to access a live-view . . . . Police in Rialto want to . . . pull up security camera feeds from cameras in [any] radius, tracking anyone who moves through those zones."); *see id.* ("In Rialto, the police have access to over 150 livestreams across restaurants, gas stations, and private residential developments . . . .").

102. Taliaferro, *supra* note 99.

103. Stein, *supra* note 24 (describing the investigative power of video analytics on New Orleans camera systems); Kwet, *supra* note 78 ("Object recognition can recognize faces, animals, cars, weapons, fires, and other things, as well as human characteristics like gender, age, and hair color.").

This human monitoring is different and distinct from automated monitoring with video analytics capturing, sorting, categorizing, and storing all the digital footage. While an observer watching the police officer stare at the video screens might not notice anything different, there is a different act occurring. With automated video analytics, all the footage being observed by the police officer is also being digitally identified, sorted, and stored in a database as it comes into the frame.[104] As will be discussed, video analytics is turning monitoring into a form of automated data capture. This distinction between video surveillance and video analytics will become central to the Fourth Amendment analysis.[105]

For police, monitoring with video analytics enabled is a game-changing power, essentially giving police eyes everywhere there are cameras and a memory of city movements for weeks or months at a time. In a Real-Time Crime Center, software does the watching, confident that the objects and movements being captured are recorded and searchable. Law enforcement has embraced this surveillance not only for its scale to expand search capabilities but also because it reduces human police presence on the streets.[106] In theory, video analytics provides public safety with less police presence.

*2. Investigation Through Retrospective Queries*.—Many times, police receive a report of a completed crime (a robbery, car theft, etc.) and need to investigate. In the investigation situation, police will use the analytical capabilities of stored video to search for images from the relevant location and time.[107]

Again, two forms of video investigation are possible. In the first, a human police officer can just roll back the video to find the images of an incident. If a 911 caller reports a robbery at the corner of 4th Street and Main Street at 2:00 PM, police can just find the relevant video feed at that time and location and watch the footage.[108] These are the same capabilities police have had for years, not too dissimilar to an old-school detective rewinding a VHS tape to observe the relevant part of the stored surveillance footage.

---

104. Lizzi Goldmeier, *Object Detection and Identification in Video Analytics*, BRIEFCAM (Mar. 23, 2022), https://www.briefcam.com/resources/blog/object-detection-and-identification-in-video-analytics/ [https://perma.cc/W9UF-FUC4].

105. See *infra* section III(A)(1).

106. Kerravala, *supra* note 92.

107. Heather Kelly & Rachel Lerman, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, WASH. POST (June 3, 2020, 7:00 AM), https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/ [https://perma.cc/53ZG-9YKA].

108. *Video Analytics Solutions for Post-Event Investigations*, BRIEFCAM, https://www.briefcam.com/solutions/police-investigations/ [https://perma.cc/JZ2L-KZPW].

In the second situation, police can investigate the incident using the analytical power of the stored digital images.[109] Essentially, the entire city under video surveillance has been captured in digital code, and police have the capacity to find a particular object within the data.[110] If that object is a person who committed a robbery, police have the ability to both search via date and time, or for a particular description, or both. Police can identify a suspect and then track that suspect back in time. In addition, police can superimpose images from different times in the same image, so objects can be compared quickly.[111]

A rather sensational example happened in Chicago, when the actor Jussie Smollett became the "victim" of an alleged racially motivated hate crime, only to be caught in the lie after police reviewed the BriefCam video analytics.[112] The story began with Smollett—a Black, gay star of the TV show *Empire*—alleging that he was assaulted by two masked men who put a noose around his neck and shouted racial and homophobic epithets.[113] The shocking allegations drew national headlines and police attention. The alleged incident was not caught on video, but police were able to identify suspects from the network of surveillance cameras in Chicago.[114] As was described by the chief of the Chicago Police Department's technology section, "[v]ideo from inside the vehicle, along with a series of public and private cameras on the North side of the city, allowed investigators to track the subject's movement backwards to where they came from prior to the attack, which ultimately led to their identification."[115] It was then that the story fell apart and it turned out that Smollett had paid the two men to stage the assault.[116] Evidence detailing their involvement in the hoax led to

109. *See* Milestone Systems, *Hartford Crime Center Expands Surveillance*, YOUTUBE (Dec. 12, 2017), https://www.youtube.com/watch?v=OlGxTITe6dE [https://perma.cc/7F8W-T6DW] (describing search capabilities of BriefCam software).

110. *Id.*; *see* Asher-Schapiro, *supra* note 23 ("For over a decade, larger U.S. cities have been building integrated monitoring programs that often link public and private cameras to allow police to keep tabs on various locations."); *see also id.* ("The number of public and private surveillance cameras in use grew from 70 million in 2018 to 85 million in 2021 . . . .").

111. Kwet, *supra* note 78 ("[I]f several people walked past a camera at 12:30 p.m., 12:40 p.m., and 12:50 p.m., BriefCam will aggregate their images into a single scene. Investigators can view all footage of interest from a given day in minutes instead of hours.").

112. Newcombe, *supra* note 93.

113. People v. Smollett, 230 N.E.3d 780, 794 (Ill. App. Ct. 2024).

114. *Analytics in Action: Safe Cities*, BRIEFCAM, https://cdn2.hubspot.net/hubfs/3916087/Resources/BriefCam%20At%20Work%20in%20Safe%20Cities.pdf [https://perma.cc/52NS-VECE].

115. *Id.*

116. Webber, *supra* note 97.

criminal charges against Smollett.[117] This type of *ex post* video investigation can happen any time after an incident has been brought to the attention of police.

Similar searches can be done with clothing, cars, license plates, or really any object. Once an object is identified, then the same (or similar objects) can be identified in the collected video data. For cases like the Smollett investigation, this meant police had a time machine of sorts to go back and search the city for clues.[118] In addition to this retrospective power, police can aggregate different data points of location and activity across time. Again, the tracking capacities are not limited to linear searches of point to point but can find all of a particular object (e.g., blue cars) in the city. The images can be superimposed on the screen so multiple objects can be viewed simultaneously.[119] Because location allows inference about identity (home, work, and friends' addresses provide clues) this locational detail can be enough for police to identify individuals wanted for questioning in criminal investigations. After all, if you know where someone sleeps at night, it is easy to figure out who they are and their other personal details.[120]

*3. Anomaly Detection and Alerts*.—The third way police use video analytics is to identify anomalies in city patterns that might be suggestive of criminal activity. Anomaly detection is a type of surveillance that looks for suspicious activities or omissions.[121] An example might be movement in an alley that usually receives no foot traffic at night or a car left in a parking lot after closing. In these cases, the expected visual scene is disturbed by

117. *Id.* ("Police tapped into Chicago's vast network of surveillance cameras—and even some homeowners' doorbell cameras—to track down two brothers who later claimed they were paid by "Empire" actor Jussie Smollett to stage an attack on him, the latest example of the city's high-tech approach to public safety.").

118. *Cf.* Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 950–51 (2016) (describing cell phones as "time machines" because they store vast amounts of information about the owner across time).

119. *See supra* notes 109–111 and accompanying text.

120. In a fascinating article, the New York Times used geolocation data from phones to identify people from otherwise anonymized data. Because everyone eventually returned to their homes, it was easy to identify a phone through its travels. Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/8PDT-S9MN].

121. Kwet, *supra* note 78 ("Anomalous or unusual behavior detection works by recording a fixed area for a period of time—say, 30 days—and determining 'normal' behavior for that scene. If the camera sees something unusual—say, a person running down a street at 3:00 a.m.—it will flag the incident for attention.").

something that does not fit the preprogrammed pattern, and an alert is signaled.[122]

Anomaly detection is not yet used in many policing systems because making predictions about citywide patterns can be difficult.[123] To work well, city environments would need to be predictable enough to predetermine what a suspicious event might look like ahead of time.[124] Across an entire city, that is a difficult request for computer programmers needing to design the suspicious anomalies at the front end. At present, particular areas—like a park or parking lot—are more likely to see anomaly detection for movements in use because the trigger is just movement when there is not expected to be any movement.[125] Although there have been a few pilot projects tested to identify suspicious actions (like actions consistent with a robbery), this pure algorithmic suspicion has not yet developed into mainstream use.[126]

The promise, however, is quite attractive. For example, imagine if police wished to discover the culprit of an illegal dumping operation along a river. Stationing police officers along a river for weeks might be too time-consuming and expensive,[127] but setting up automated alerts for trucks along the banks of the river might be easy enough.[128] Or imagine police are concerned about a particular symbolic statue being vandalized but, again, do not have the capacity to have individual officers personally protect the statue. Establishing a video analytics system to alert for activity around the statue might prevent vandalism (and/or catch the suspects).

---

122. Niraj Chokshi, *How Surveillance Cameras Could be Weaponized with AI*, N.Y. TIMES (June 13, 2019), https://www.nytimes.com/2019/06/13/us/aclu-surveillance-artificial-intelligence.html [https://perma.cc/B7EK-8A2W] ("Advancements in artificial intelligence could supercharge surveillance, allowing camera owners to identify 'unusual' behavior, recognize actions like hugging or kissing, easily seek out embarrassing footage and estimate a person's age or, possibly, even their disposition . . . ." (citing Stanley, *supra* note 7)).

123. *But see, e.g.*, Mert Karakaya, *How ViTs/ChatGPT Can Automatically Alert on Protests Tested*, IPVM (April 29, 2024, 8:12 AM), https://ipvm.com/reports/vits-protests [https://perma.cc/QTS5-BDPQ] (showing how protest-monitoring technologies are now being tested).

124. *See* Maass & Guariglia, *supra* note 72 ("Avigilon has a pair of algorithms that it uses to predict what it calls 'unusual events.' The first can detect 'unusual motions,' essentially patterns of pixels that don't match what you'd normally expect in the scene. . . . The second can detect 'unusual activity' involving cars and people."); Quinlan, *supra* note 2 ("While traditional police work is reactive, law enforcement's access to a continual feed of video and data makes proactive policing a growing possibility.").

125. *See* Maass & Guariglia, *supra* note 72 (describing how video analytics can identify even small movements and changes to an image).

126. *See generally* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 873 (2016).

127. *See* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 337 (2014) (showing how the reduction of costs arising from technologically enhanced surveillance alters expectations of privacy).

128. *See* Erin Tracy, *supra* note 9 (discussing the use of anomaly detection to identify people who dump trash along a roadway).

In addition, anomaly detection is valuable as a public safety measure exposing abandoned bags and other suspicious packages.[129] Because of terrorism threats, police are concerned with bags that might hold explosives or other dangerous material. Anomaly detection of bags is used in airports, bus stations, subways, and other potential mass transit targets, but could be used across the city environment.[130]

Finally, in the not-too-distant-future we will see "crimes" alerted to as anomalies using AI-large language models (LLMs). For example, researchers have fed Ring video cameras into AI systems like ChatGPT-4, Gemini 1.0, and Claude 3 Sonnet and asked the systems whether they could identify a crime and whether the police should be called.[131] Once developed as a capability, this will give RTCC systems the ability to identify crimes from visual clues without human involvement. Unfortunately, the early tests show a lack of uniformity in the results, meaning that depending on the LLM system a city uses, there might be different crime alerts from the same underlying actions.[132] Further, error concerns emerge, as video analytics might confuse a tackle football game with a fight or a stickball bat with a weapon.[133]

All the above use cases, however, must be qualified by the concern that police might use the technologies in different ways against different communities.[134] Race and racialized policing have been a part of policing technology since its creation.[135] The use of new video analytics surveillance

129. Of course, the number of streets and potential for false alarms grows in a city space. As a result, again such anomaly detection is better used in particular locations with more predictable patterns of behavior.

130. *See supra* note 87 and accompanying text.

131. Shomik Jain, D. Calacci & Ashia Wilson, *As an AI Language Model, "Yes I Would Recommend Calling the Police": Norm Inconsistency in LLM Decision-Making*, ARXIV (May 2024), https://arxiv.org/pdf/2405.14812 [https://perma.cc/R47U-SRNR] ("[W]e prompt GPT-4, Gemini, and Claude with real videos from the Amazon Ring Neighbors platform and test (1) whether models state that a crime is happening and (2) whether they recommend calling the police.").

132. *Id.* (finding that "all models exhibit norm inconsistency" in identifying when to call the police).

133. *But see* Karakaya, *supra* note 123 (demonstrating how early tests of vision transformer that can identify events from video can distinguish between a fight and a dance party).

134. *See* Vincent M. Southerland, *The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies*, 70 UCLA L. REV. 2, 17–18 (2023) (describing how marginalized communities experience police technologies as tools of racial control). *See generally* FERGUSON, *supra* note 39 (exploring the intersection between opaque "data" in data-driven policing and the racialized criminal justice system).

135. *See* Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1111–16 (2020) (arguing that contemporary police surveillance in Baltimore is rooted in the history of chattel slavery); Ngozi Okidegbe, *When They Hear Us: Race, Algorithms and the Practice of Criminal Law*, 29 KAN. J.L. & PUB. POL'Y 329, 332–34 (2020) (explaining that "currently employed algorithms reproduce the racial status quo"); Mary Anne Franks, *Democratic Surveillance*, 30

cannot avoid those same concerns. Where the cameras are placed, who uses them, for what crimes, and why are all intertwined with structural critiques of policing in America. The lens of video analytics cannot filter out the reality of race and surveillance, and courts need to confront the inequalities in application.

## II. Video Analytics and the Search Question

In the same way video analytics offers a different way to understand the observable world, computer vision also offers a different way to understand the Fourth Amendment search doctrine. Or, in the constitutional language that controls the Fourth Amendment doctrine, video analytics alters the reasonable expectation of privacy analysis.[136]

### *A. The Search Question*

The Fourth Amendment prohibits "unreasonable searches and seizures."[137] The result of this textual command has been a focus on the threshold questions of whether a government agent has searched or seized something and the reasonableness with which the search or seizure was conducted.[138] A "search" is a term of art in Fourth Amendment doctrine defined either as a violation of a "reasonable expectation of privacy"[139] or a physical intrusion into a constitutionally protected space with the intent to gather information.[140] If a search occurs without a warrant or an exception to the warrant requirement, a Fourth Amendment violation has occurred.[141] If

HARV. J.L. & TECH. 425, 441–43 (2017) (articulating the history of surveillance on Black Americans); Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 166 (2021) (describing how police technology can exacerbate racial inequities). *But see* I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1280 (2017) (arguing that police use of technology should be increased and that increased surveillance overall is preferable for racial equity).

136. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (suggesting a reasonable expectation of privacy test).

137. U.S. CONST. amend. IV.

138. Although, as any Fourth Amendment scholar knows, the textual command has generated many non-textual tests in application. Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 240 (2019) (discussing how a textualist approach might simplify Fourth Amendment analysis when compared to current Supreme Court practice).

139. *Katz*, 389 U.S. at 361 (Harlan, J. concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

140. United States v. Jones, 565 U.S. 400, 404–05 (2012) (describing a search as a physical intrusion with the intent to gather information).

141. Arizona v. Gant, 556 U.S. 332, 338 (2009) ("[O]ur analysis begins . . . with the basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" (quoting *Katz*, 389 U.S. at 357)).

the governmental act is not considered a search, the Fourth Amendment is not implicated, and no constitutional analysis is needed.

The reasonable expectation of privacy test has confused generations of lawyers and unsettled judges, academics, and pretty much everyone who ever tried to figure out whether there was an expectation of privacy in a place, activity, or thing.[142] The test has served the purpose of allowing judges to draw lines around Fourth Amendment freedoms and law professors to critique that line-drawing but has largely managed to dissatisfy almost everyone in practice.[143] Yet, it is the existing law and must be addressed by any judge or lawyer faced with a case involving police surveillance powers.

The core question presented by video analytics (as with other surveillance technologies) is how to understand expectations of privacy in public in the face of technologies that erode such privacy.[144] Do you—walking down the street in Chicago—have a reasonable expectation of privacy in your location, actions, patterns, etc.? How do we know? Is it a normative or empirical judgment? Does it depend on what or who you expect will be watching? Does it matter how long people are watching? Does it matter what inferences can be drawn about your activities? Is it a function of the observational technological tool or the systemic nature of collection? Does scale or scope of the observation matter? These questions are key to understanding the doctrinal tension in the law addressed below.

The Seventh Circuit Court of Appeals began its decision in *United States v. Tuggle*[145]—a case involving long-term digital pole cameras—by framing the reasonable expectation of privacy question in rather vivid terms:

> One day, in a not-so-distant future, millions of Americans may well wake up in a smart-home-dotted nation. As they walk out their front doors, cameras installed on nearby doorbells, vehicles, and municipal traffic lights will sense and record their movements, documenting their departure times, catching glimpses of their phone screens, and taking note of the people that accompany them.

---

142. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 861 (2016) ("[I]t is never clear *ex ante* what the Supreme Court will find to be a reasonable expectation of privacy.").

143. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence."); Carpenter v. United States, 138 S. Ct. 2206, 2236 (2018) (Thomas, J., dissenting) ("The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence.").

144. This expectation also may be impacted by racial bias or social economic status. *See* Arnett, *supra* note 135, at 1140 (describing the disparate effect of the distinction the Fourth Amendment precedent draws between public and private space which "rests in part on a privileged concept of privacy, one much divorced from the realities of freedom and safety which also impact privacy").

145. 4 F.4th 505 (7th Cir. 2021), *cert. denied* 142 S. Ct. 1107 (2022).

> These future Americans will traverse their communities under the perpetual gaze of cameras. Camera-studded streets, highways, and transit networks will generate precise information about each vehicle and its passengers, for example, recording peoples' everyday routes and deviations therefrom. Upon arrival at their workplaces, schools, and appointments, cameras on buildings will observe their attire and belongings while body cameras donned on the vests of police and security officers will record snippets of face-to-face or phone conversations. That same network of cameras will continue to capture Americans from many angles as they run errands and rendezvous to various social gatherings. By the end of the day, millions of unblinking eyes will have discerned Americans' occupations and daily routines, the people and groups with whom they associate, the businesses they frequent, their recreational activities, and much more.
>
> The setting described above is not yet a total reality. Nonetheless, we are steadily approaching a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans.[146]

The Seventh Circuit Court of Appeals declined to resolve the constitutional questions raised in its hypothetical surveillance dystopia (beyond the points needed to resolve the case),[147] but the tenor of the passage reveals the court's concern about future claims of privacy in public.

The open constitutional question—as applied to video analytics systems—is whether use of such systems is a "search" for Fourth Amendment purposes. And, more specifically, is video analytics *monitoring* a search? Is video analytics *investigation* a search? Is *anomaly detection* a search? If the answer is yes to any (or all) of the questions, then this governmental action without a warrant or applicable exception would be considered unreasonable and a Fourth Amendment violation.

### *B. The Traditional Canon of Fourth Amendment Search Cases*

To answer the question of whether video analytics in Real-Time Crime Centers is a search, one must understand the background Fourth Amendment doctrine. In a series of cases from the 1960s to the 1990s, the Supreme Court initiated a conversation about expectations of privacy in public. In what I call "the traditional canon," the Court explored rather low tech, analog surveillance technologies to hold that people could expect little privacy in public.[148]

---

146. *Id.* at 509.

147. *Id.* at 528–29.

148. Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 79 (2013) (recognizing that

The canon is centered by *Katz v. United States*, the case that gave us the "reasonable expectation of privacy" test.[149] To investigate whether Charlie Katz was engaged in illegal gambling, the FBI attached a tape recorder to the roof of a coin-operated, glass-enclosed phone booth.[150] Katz's conversations were recorded, and he moved to suppress the evidence as a violation of the Fourth Amendment. In holding that the police needed a warrant to listen to Katz's conversation, the Supreme Court distinguished between the private nature of the phone call and Katz's public presence in the phone booth.[151] The Court held that a person could claim a reasonable expectation of privacy in their conversation in a telephone booth because they had paid the toll to use the phone, but that they might not be able to claim an expectation of privacy from observations of their physical presence in the phone booth.[152] In the Court's words, "For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[153] In other words, it might be reasonable to think that one's phone call was not being listened to by police, but anyone (even police) could see someone using the phone with their own two eyes.

This traditional logic—that one could expect little privacy in publicly observable places—expanded in two cases involving police surveillance using aerial technology. The question in both cases was whether a homeowner had a reasonable expectation of privacy in areas that could be observed from a public vantage point. In *California v. Ciraolo*,[154] police used a fixed-wing plane to fly over Ciraolo's property and observed illegal

"police surveillance in public has traditionally been entirely outside the Fourth Amendment's coverage"); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 497 (2006) ("[T]he Court has concluded that while the Fourth Amendment protects against surveillance in private places such as one's home, the Amendment has little applicability to surveillance in public places.").

149. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (suggesting a reasonable expectation of privacy test).

150. Brief for Petitioner at 5, *Katz*, 389 U.S. 347 (No. 35) ("Petitioner's conversation was overheard and recorded [and later transcribed] by means of a tape recorder which was placed on top of the middle booth. One of the three booths was placed out of order by the FBI with the consent of the telephone company." (citations omitted)).

151. *Katz*, 389 U.S. at 352 ("[W]hat he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen.").

152. *Id.* at 352 ("One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

153. *Id.* at 351–52.

154. 476 U.S. 207 (1986).

marijuana plants.[155] The Supreme Court held that Ciraolo could expect no privacy in areas observable to the public by human eyesight; "The Fourth Amendment simply does not require the police traveling in the public airways at [a 1,000 foot] altitude to obtain a warrant in order to observe what is visible to the naked eye."[156] *Ciraolo* was followed by *Florida v. Riley*[157] which involved police using a helicopter flying at 400 feet to observe illegal marijuana growing in Riley's backyard.[158] In *Riley*, a plurality held that Riley failed to demonstrate that his expectation of privacy in his backyard was reasonable.[159] In both cases, the fact that otherwise private information had been knowingly exposed to public observation undermined any reasonable expectation of privacy.

The traditional "no privacy in public" logic was further extended in *United States v. Knotts*,[160] which involved the use of a radio beeper to track a car in public.[161] The question in *Knotts* was whether someone could claim a violation of an expectation of privacy after being tracked by an electronic

---

155. *Id.* at 209 ("[The officers] secured a private plane and flew over respondent's house at an altitude of 1,000 feet . . . . Both officers were trained in marijuana identification. From the overflight, the officers readily identified marijuana plants 8 feet to 10 feet in height growing in . . . respondent's yard.").

156. *Id.* at 215.

157. 488 U.S. 445 (1989).

158. *Id.* at 448. Justice White, writing for the plurality, summarized the facts of the case:

> When an investigating officer discovered that he could not see the contents of the greenhouse from the road, he circled twice over respondent's property in a helicopter at the height of 400 feet. With his naked eye, he was able to see through the openings in the roof and one or more of the open sides of the greenhouse and to identify what he thought was marijuana growing in the structure.

*Id.*

159. *Id.* at 451–52. *Riley* involved a plurality opinion with the controlling concurrence written by Justice Sandra Day O'Connor that focused on the defendant's failure to prove that helicopters were unusual in the area:

> In determining whether Riley had a reasonable expectation of privacy from aerial observation, the relevant inquiry after *Ciraolo* is not whether the helicopter was where it had a right to be under FAA regulations. Rather, consistent with *Katz*, we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not "one that society is prepared to recognize as 'reasonable.'"

*Id.* at 454 (O'Connor, J. concurring) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

160. 460 U.S. 276 (1983).

161. *Id.* at 285. Justice Rehnquist summarized the facts of the case:

> In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of respondent's codefendants. By monitoring the progress of a car carrying the chloroform Minnesota law enforcement agents were able to trace the can of chloroform from its place of purchase in Minneapolis, Minn[esota], to respondent's secluded cabin near Shell Lake, Wis[consin].

*Id.* at 277.

beeper.[162] In upholding the use of a beeper to track suspected drug manufacturing materials, the Supreme Court stated, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[163] Further, the Court expressly allowed for technologically enhanced visual surveillance in public.

> Visual surveillance from public places along Petschen's route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[164]

Together, these statements have been read to find that individuals in public have little expectation of privacy from police observation—including video surveillance.[165]

The final piece of the traditional "no privacy in public" logic is orthogonal in nature, involving related claims about losing privacy when information is voluntarily shared with third parties.[166] While not focused on physical presence in public, in two different lines of cases, the Supreme Court has essentially created a voluntary disclosure doctrine reasoning that by taking an action that exposes private matters to a third party, the individual forfeits a claim to expectations of privacy against other people. For example, with bank records and home phone records, the Court has held that a customer's voluntary disclosure of information to a third party (bank or phone company) also demonstrates a lack of any expectation of privacy in that information *vis-à-vis* the government.[167] Similarly, the Supreme Court has held that disclosures to third party individuals who later convey that information to the police carry no reasonable expectation of privacy.[168] Such

---

162. *Id.* at 285.

163. *Id.* at 279, 281.

164. *Id.* at 282.

165. Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 1975–76 (2018) ("U.S. Supreme Court precedent establishes that citizens do not generally enjoy a reasonable expectation of privacy in public.").

166. *See* Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 829–30 (2022) (discussing development of the third-party doctrine); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 575–77 (2009) (explaining reasons for the third-party doctrine).

167. Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (third party land line phone records); United States v. Miller, 425 U.S. 435, 437 (1976) (third party bank records).

168. United States v. White, 401 U.S. 745, 746–47, 749 (1971).

"false friend" and "private search" cases also support the argument that voluntary public exposure of private information undermines any claim to an expectation of privacy.[169]

The traditional Fourth Amendment canon is still controlling law and used by courts to decide issues of twenty-first century surveillance.[170] In fact, courts have ignored some of the limits and nuances of the rulings, allowing wide-spread use of policing technologies under the theory that almost anything goes when it comes to public surveillance.[171] Based on this interpretation, police chiefs have publicly stated that most surveillance is allowed in public without constitutional restraint.[172] This justification also has been used to surveil poor communities of color deemed "high crime" more than other communities.[173]

Read carefully, however, the Supreme Court's doctrine on privacy in public is more nuanced, justifying the analog surveillance technologies of the twentieth century but not necessarily validating mass surveillance systems that have arisen in the twenty-first century like nationwide cell-site location systems, sprawling GPS systems, or citywide Real-Time Crime Centers. It is

169. *See* Donald L. Doernberg, *"Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253, 279–82 (2006) (discussing false friend cases); Wayne A. Logan, *Crowdsourcing Crime Control*, 99 TEXAS L. REV. 137, 154–55 (2020) (discussing the private search doctrine).

170. The *Tuggle* case discussed earlier is a good example. *See supra* notes 145–147 and accompanying text. The Seventh Circuit Court of Appeals clearly articulated the dangers of a growing video surveillance state and voiced the need for expanded protection and yet felt compelled to interpret existing precedent about little privacy in public. United States v. Tuggle, 4 F.4th 505, 509–11 (7th Cir. 2021) ("Ultimately, bound by Supreme Court precedent and without other statutory or jurisprudential means to cabin the government's surveillance techniques presented here, we hold that the extensive pole camera surveillance in this case did not constitute a search under the current understanding of the Fourth Amendment.").

171. As just one stark example, in a case involving the Baltimore Police Department's use of the Persistent Surveillance System airplanes, which could videotape the entire city and record all objects below for twelve hours at a time, the trial court merely analyzed the traditional overflight cases. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 704, 712–13 (D. Md. 2020), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021). Obviously, the scale, scope, and privacy expectations might be different with such new powerful technology, but the trial court followed existing precedent. *See* Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 47–48 (2022) (critiquing this myopic analysis).

172. *See, e.g.*, Paul Edward Parker, *Who's Watching You? New Surveillance Cameras Make Inroads in RI, Raising Privacy Concerns*, PROVIDENCE J. (Feb. 12, 2022, 5:00 AM), https://eu.providencejournal.com/story/news/local/2022/02/12/rhode-island-police-surveillance-camera-network-raises-privacy-concerns/6683184001/ [https://perma.cc/9UNZ-WGYY] (quoting Col. Michael J. Winquist, the police chief in Cranston as saying, "[w]hen you're on a public roadway, there's no expectation of privacy").

173. *See* Chaz Arnett, *Black Lives Monitored*, 69 UCLA L. REV. 1384, 1406 (2023) (recounting the leniency given to law enforcement to fight the "War on Drugs"); Arnett, *supra* note 135, at 1140 (noting the history of racially biased surveillance in the United States); Monica C. Bell, *Anti-Segregation Policing*, 95 N.Y.U. L. REV. 650, 710 (2020) (emphasizing that policing plays an "outsized role" in designating certain neighborhoods as high crime).

for that reason, perhaps, that the Supreme Court has tried to articulate a different set of principles in digital surveillance cases that offer a "qualitatively different" privacy threat.[174]

### *C. The "Digital Is Different" Cases*

In three more recent cases, the Supreme Court has hinted that "digital is different" when it comes to police searching for digital clues.[175] The cases do not offer a new test; rather, they purport to be interpreting the reasonable expectation of privacy test, but they do suggest a more protective approach to privacy. Two of the cases, *United States v. Jones*[176] and *Carpenter v. United States*,[177] directly confront expectations of privacy in public.

In *Jones*, the Supreme Court addressed whether affixing a GPS tracking device on a car and recording tracking data for twenty-eight days was a search for Fourth Amendment purposes.[178] The majority resolved the issue on a trespass theory, holding that the placement of the GPS device on the car was a physical intrusion with the intent to gather information and thus a search.[179] This holding did not address whether Antoine Jones had a reasonable expectation of privacy from not being tracked for twenty-eight days.[180] Five concurring justices did, however, address whether Jones' public movements could be tracked via GPS for twenty-eight days without a

174. State v. Briggs, 283 A.3d 165, 168–69 (N.J. Super. Law. Div. 2019) ("The Carpenter Court distinguished *Miller* and *Smith* on the basis that CSLI is 'qualitatively different' from telephone records and bank records as CSLI 'chronicles a person's past movement through the record of his cell phone signals' and it is obtained without an 'affirmative act on the user beyond powering up.'" (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217–17 (2018))).

175. In some ways, focusing on the term "digital" is misleading in that digital is just the prerequisite for the changes in scale, scope, quantitative, and qualitative differences that arise from mass collection of digital information. I use the term "digital" as a shorthand for the change from analog policing tools to digital policing systems, recognizing that the issue is not just how the information is collected and processed (digitization), but what can be done with it (datafication). "[Digitization] refers to the use of computing devices to record, quantify, format, or store data as a series of digits. In contrast, 'datafication' refers to 'long-term storage in a format that is searchable, computationally manipulable, and [that] may be aggregated with information from other' sources." Ira S. Rubinstein & Bilyana Petkova, *Governing Privacy in the Datafied City*, 47 FORDHAM URB. L.J. 755, 759 (2020) (quoting Katherine Strandburg, *Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 5, 11 (2014)).

176. 565 U.S. 400 (2012).

177. 138 S. Ct. 2206 (2018).

178. *Jones*, 565 U.S. at 402–03.

179. *Id.* at 404–05 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

180. *Id.* at 412–13.

warrant.[181] In two concurring opinions, the justices recognized that long-term tracking—even in public—violated a reasonable expectation of privacy.[182] While it is true that police could have physically followed Jones' car in public for the same amount of time, the justices recognized that technology changed reasonable expectations of privacy and determined that the long-term GPS surveillance was a search.

This understanding that tracking public movements might infringe on a reasonable expectation of privacy was confirmed in *Carpenter v. United States*.[183] *Carpenter* asked whether an individual had a reasonable expectation of privacy from being tracked for seven days by cell-site location information (CSLI).[184] CSLI is the location data phone companies use to monitor cell phones and connect them with nearby cell phone towers.[185] CSLI generates an approximate triangulated location of the cell phone user at all times.[186] In *Carpenter*, police had requested that cell phone companies turn over weeks' worth of CSLI on Timothy Carpenter, who was suspected of masterminding a string of robberies.[187] The CSLI placed Carpenter at the robbery locations at the time of the crimes.[188] Carpenter argued that this collection of location data without a warrant violated his reasonable expectation of privacy and thus the Fourth Amendment.[189]

The Supreme Court agreed with Carpenter, holding that long-term location tracking violated a reasonable expectation of privacy and required a warrant.[190] This was true even though Carpenter's movements were in public.[191] This was true even though the data had been provided to a third

181. *Id.* at 415–16 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); *id.* at 427, 430 (Alito, J., concurring in the judgment).

182. *Id.* at 430 (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

183. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*.").

184. *Id.* at 2211.

185. Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 497–98 (2017) (describing the technological and legal issues in *Carpenter*).

186. *Id.*

187. *Carpenter*, 138 S. Ct. at 2212.

188. *Id.* at 2212–13.

189. *Id.* at 2212.

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

191. All of the locations revealed were outside of Carpenter's home or private property. *See id.* at 2232 (Kennedy, J., dissenting) (noting that the CSLI records at issue covered Carpenter's location within "an area covering between around a dozen and several hundred city blocks").

party (the cellphone company).[192] This was true even though nothing more than his location at the robbed stores was to be introduced at trial.[193] In contrast to the traditional canon of cases, the *Carpenter* court adopted the reasoning of the *Jones* concurrences and recognized that the digital surveillance power of location tracking required a different analysis, even in public.[194]

These two "digital-*Katz*" cases[195] will be addressed in more detail in Part III, but they represent a break in how the Supreme Court has traditionally addressed privacy in public. They represent a new line of analysis about how the Court approaches the tracking of movements from one place to another. They also stand in tension with the traditional canon of cases, leaving many unanswered questions.

The final piece of the "digital is different" line of cases is *Riley v. California*.[196] *Riley* involved the warrantless search of a smartphone incident to arrest.[197] In reaching its conclusion, the Court explored the difference between analog searches and digital searches.[198] David Riley was arrested for a traffic offense and had his car impounded.[199] During a routine inventory search of the car, two guns were recovered.[200] Without a warrant, detectives investigating Riley searched through his smartphone for evidence connecting him to criminal activity.[201] In the photo app in Riley's smartphone, police found a photograph that prosecutors used to link him to an earlier shooting.[202] Riley filed a motion to suppress the data from his smartphone arguing that police needed a warrant to search the smartphone.[203]

192. The records at issue were held by private cellphone companies that provided cellphone services to paying customers. *Id.* at 2212.

193. *Id.* at 2212–13.

194. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see id.* at 2217–18 ("In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*."); *see also* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 359 (2019) (interpreting what *Carpenter* means for other technologies).

195. Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://harvardlawreview.org/blog/2018/06/future-proofing-the-fourth-amendment/ [https://perma.cc/L822-Y6LL].

196. Riley v. California, 573 U.S. 373 (2014).

197. *Id.* at 378–79.

198. *Id.* at 400–01.

199. *Id.* at 378.

200. *Id.*

201. *Id.* at 378–79.

202. *Id.* at 379.

203. *Id.*

The Supreme Court agreed with Riley, holding that a warrant was required to search a digital device even incident to arrest.[204] In coming to this conclusion, the Court distinguished analog search cases that had allowed police to search any physical objects recovered on an arrestee incident to arrest.[205] The Court considered the privacy harms of a smartphone different than a wallet or cigarette pack recovered incident to arrest.[206] The Court specifically described why exposing data in a smartphone was qualitatively and quantitatively different from any analog cases.[207] Data in a smartphone included contacts, calendars, notes, email, texts, financial information, photos, news, other apps, and internet searches (among other things).[208] In statements that acknowledged both the scale and scope of digital evidence in most smartphones and the complexity around data being both in a smart device and in the cloud, the Court recognized that digital searches should be treated differently than their analog equivalents.[209] In Riley's case, that meant that police needed a warrant.[210]

### *D. Unexamined Fourth Amendment Search Questions*

Before moving on to apply the Fourth Amendment doctrine to the puzzle of video analytics in Part III, it is worth highlighting a few of the unstated assumptions behind the Supreme Court's traditional canon. In simplified form, the Court has generally assumed that the threat of police searches comes from human police officers, using simple surveillance tools, limited by temporal realities, and involving a singular search act. These four

204. *Id.* at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

205. *Id.* at 386 ("But while *Robinson*'s categorical rule [allowing searches incident to arrest] strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.").

206. *Id.* at 393–94 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. . . . Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read . . . ."); *see id.* at 400 ("[T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery.").

207. *Id.* at 393–94 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

208. *Id.* ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as telephones. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

209. *Id.* at 396–97 (concluding that because "[a] phone . . . contains in digital form many sensitive records previously found in the home . . . [and] a broad array of private information never found in a home in any form," cell phone searches "typically expose the government to far *more* than the most exhaustive search of a house").

210. *Id.* at 401 ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").

insights will be helpful later to resolve some of the tensions arising between the traditional canon and the "digital is different" cases.

Traditionally, Fourth Amendment expectations of privacy have been judged against human observations. In other words, courts examine reasonable expectations by looking at whether a reasonable person can guard their privacy against what they think a human being can do to invade that privacy.[211] Implicit in *Katz*, and explicit in *Ciraolo*, *Riley*, and *Knotts*, was the human police officer observing with their "naked eye" (even if augmented by planes, helicopters, or beepers).[212] The logic makes some sense. By being in public, one can expect to be observed by human police officers. Especially in an era before digital surveillance systems, the only expectations of surveillance one might have reasonably had came from or was related to human beings. In 1967, if one wanted to guard one's privacy, one could do so against existing human capabilities. In the analog, human-centric era of those cases, it made good sense to delimit expectations around possible human invasions and observations (not imaginary technologies that did not yet exist). However, *Carpenter* and *Jones* hint at the recognition that automation and non-human capacities change the balance of police power and require greater protections.[213] As Justice Alito acknowledged in *Jones*,

211. Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 853 (2022) (noting how a reasonable expectation of privacy in early Fourth Amendment cases was dependent on expectations in relation to human observation).

212. California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The observations by Officers Shutz and Rodriguez in this case took place within public navigable airspace . . . in a physically nonintrusive manner; from this point they were able to observe plants readily discernible to the naked eye as marijuana."); Florida v. Riley, 488 U.S. 445, 448 (1989) ("[A]n investigating officer . . . circled twice over respondent's property in a helicopter at the height of 400 feet. With his naked eye, he was able to see through the openings in the roof . . . of the greenhouse and to identify what he thought was marijuana . . . ."); *compare Riley*, 488 U.S. at 450 ("The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye." (quoting *Ciraolo*, 476 U.S. at 215)), *with* United States v. Knotts, 460 U.S. 276, 285 ("But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

213. *Carpenter*, in fact, speaks explicitly about the danger of a mechanical application of analog precedent. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 ("[W]e rejected in *Kyllo* a 'mechanical interpretation' of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search."); *see also* Kate Weisburd, *Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring*, 98 N.C. L. REV. 717, 721 (2020) ("The Court has likewise recognized that the concept of a 'reasonable expectation of privacy' for Fourth Amendment purposes must reflect the 'seismic shifts in digital technology' that now allow for 'near perfect surveillance' of digital records that 'hold for many Americans the "privacies of life."'" (citations omitted)); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 615–17 (2011) (describing automation and what happens without human actions).

human officers could not have tracked the suspect as effortlessly before GPS because they did not have the real-world capabilities to do so.[214]

Second, expectations of privacy have traditionally responded to singular surveillance "tools," and thus courts did not develop a language for the scale, scope, and aggregation harms of modern mass surveillance systems.[215] All of the cases in the traditional canon involved surveillance tools—one-off information collection devices. Whether we are analyzing a beeper, tape recorder, thermal imager, pen register, or film camera, all the early cases involved a single-use technology that, because of technological limitations, was necessarily limited in scope and scale.[216] Systems that involve many data sources and aggregating capabilities may produce a different privacy harm.[217] Such systems are bigger, deeper, wider, richer, and more revealing than any single-use source of information. The Court in *Carpenter* recognized this reality when it came to systems of location tracking like CSLI.[218] The identified harm with CSLI was a nationwide system that could track anyone for any reason without a warrant and aggregate that data together.[219]

Third, expectations of privacy have been temporal in nature, having a natural limit on both the amount of data collected and the ability to go back in time to uncover past clues.[220] Due to the nature of analog surveillance, the temporal element tended to be assumed. Not only was it difficult and expensive to have long-term, persistent surveillance (e.g., using a constant

---

214. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

215. In prior work, I have analyzed how this distinction can make a difference in case outcomes. Ferguson, *supra* note 171, at 38–39 ("The thermal imaging device in *Kyllo* was . . . . a standalone tool . . . . Similarly, the flyover cases in *California v. Ciraolo* and *Florida v. Riley* involved ordinary cameras . . . . In contrast, the CSLI system in *Carpenter* was a vast network of cell towers . . . and the *Jones* case involved a global satellite tracking system." (citations omitted)).

216. *Id.*

217. *See generally* Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289 (2015) (discussing data aggregation cases which have led courts to depart from Fourth Amendment doctrine and thereby undermine expectations of individual privacy).

218. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("[W]hen the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.").

219. *Id.*

220. In a prior article, I called this the "anti-permanence principle":

> The anti-permanence principle involves not just the collection of data but the long-term storage and retrievability of that information. The Court in both *Jones* and *Carpenter* expressed concern about the government's ability to revisit that information for any reason and for all time. This "time-machine-like" capability to access permanently stored data produced a fear about the creation of overbroad and unlimited data systems that allow for retrospective searching.

Ferguson, *supra* note 80, at 1135–36.

hovering helicopter), but it was hard, if not impossible, to use the accumulated data retrospectively.[221] Police collected a beeper's track, or a series of conversations, or a few photos. They did not accumulate all beepers of all cars in a city, or everyone's calls, or photos of everyone that could be reviewed at any time.[222] In addition, viewing the tape of a CCTV camera took a long time because one had to watch the film in almost real time.[223] It was not easy to search for objects or people. *Carpenter* and *Jones* both recognized the retrospective nature of digital searches and attendant harms that changed the analysis.[224]

Fourth, and somewhat related to both the temporal argument and the human argument, expectations of privacy were determined in response to a particular government act.[225] It was easy to see when the contested "search" occurred. Traditionally, there was an affirmative act of a police officer that triggered the inquiry.[226] Maybe the officer entered a home, tapped a phone, or flew over a house, but one could know when the contested "search" occurred. This changes, of course, when the collection of information is

---

221. In *Carpenter*, the Court acknowledged both the unprecedented scope of information provided by retrospective data pools and the absence of equivalent historical analogs:

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years.

*Carpenter*, 138 S. Ct. at 2218.

222. *See id.* (recognizing the unprecedented scope of collecting this information, which is "continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation" and thus implicates everyone's privacy rights).

223. Kwet, *supra* note 78 ("CCTV cameras were low-resolution analog devices that recorded onto tapes. . . . Few cameras were placed in [public], and the power to track people was limited: If police wanted to pursue a person of interest, they had to spend hours collecting footage by foot from nearby locations."); BOOTH ET AL., *supra* note 42, at 8 ("Sharing [CCTV] video information with another investigator required a security team to manually retrieve a tape and transport it to the next agent, who would then spend even more time scrolling through the VHS tape.").

224. *Carpenter*, 138 S. Ct. at 2218–20; United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("The government can store such records and efficiently mine them for information years into the future." (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc))).

225. *See* Ferguson, *supra* note 171, at 17 ("Automation changes the calculus because the government is asking the technology to keep collecting continuously ('persistently'). Continually recording all of an individual's phone calls for months is a different act than capturing a few payphone conversations.").

226. *See* Tokson, *supra* note 213, at 612–14 (identifying the concept underlying most theories of "privacy harm" as the fact that personal, private, or otherwise intimate information is being relayed to a human observer).

ongoing and continuous.[227] One of the hardest and still likely unanswered questions in *Carpenter* was when did the search occur.[228] The Court discusses the "acquisition" of the data from the cell phone companies, but that is not when the information was obtained about the suspect (which happened well before police got access to it).[229] Is there no search until the government acquires the information? What if the data collection is ongoing and continuous, or directly fed in parallel to police? It is a messy problem, one that will be addressed again in Part III.

These four assumptions—implicit in the traditional canon—are directly challenged by video analytics in Real-Time Crime Centers, a non-human system of surveillance that constantly and continuously monitors people, places, and actions. How the Fourth Amendment fits that problem of computer vision is the subject of the next Part.

## III. Video Analytics and the Fourth Amendment

Video analytics involves capturing, sorting, and storing images through digital, AI-enhanced means. The question of whether someone has a reasonable expectation of privacy in public from this government surveillance system is difficult because constitutional principles from the "traditional canon" and the "digital is different" cases conflict.[230]

This Article argues that video analytics running on these citywide surveillance systems violates a reasonable expectation of privacy and is a search for Fourth Amendment purposes. Properly understood, the technology powering video analytics—be it virtual patrols, retrospective investigation, or anomaly detection—involves continuous, wide-scale, suspicionless object-recognition matching without a warrant. Put simply, to work as designed, video analytics must be searching everything, everywhere, all at

227. *See id.* at 615–16 (arguing that the Supreme Court's Fourth Amendment jurisprudence establishes that information collected via continuous technological monitoring is nevertheless "private" until it is examined by a human being); Maneka Sinha, *supra* note 75, at 596 (noting that human judgments of "reliable" information justifying a search or seizure have been supplanted by judgments made by policing technology).

228. Orin Kerr, *When Does a* Carpenter *Search Start—and When Does It Stop?*, LAWFARE (July 6, 2018, 10:24 AM), https://www.lawfaremedia.org/article/when-does-carpenter-search-start-and-when-does-it-stop [https://perma.cc/GZ2Z-HQNS].

229. *Carpenter*, 138 S. Ct. at 2221 ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

230. Many scholars have also attempted to craft Fourth Amendment arguments about a privacy in public. *E.g.*, Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 91 (2007); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 536 (2012); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 682–84 (2013).

once to pattern match and categorize the objects (including persons and effects) in its computer vision.[231]

Such a statement that video analytics in Real-Time Crime Centers is a Fourth Amendment search is admittedly bold and contestable. It essentially calls into question the continued use of this technology by police. This Part proceeds in two steps trying to back up the claim. The first subpart details what I call the "digital is different version" of the argument.[232] This first step posits that—at a minimum—courts cannot rely on the traditional analog canon to resolve the Fourth Amendment search question. The argument takes the initial half step of positing that existing Fourth Amendment precedent does not cover the puzzle of video analytics, with arguments pointing in the direction of finding a Fourth Amendment violation.

The second subpart expands this argument, asserting that video analytics powered by AI-enhanced pattern matching—properly understood—is an overbroad, generalized, and unreasonable search under the Fourth Amendment.[233] The argument explains that by design, video analytics technology cannot escape automated, large-scale, and warrantless searching, matching, and tracking of people and effects in ways that reveal the "privacies of life."[234] In other words, because of the way the AI pattern-matching technology was designed and operates, it must act as a warrantless mass surveillance system, and thus violates a reasonable expectation of privacy (at least when applied to citywide camera systems).

Both arguments suggest that the video analytics systems currently being used by police—at least those with sufficient network cameras—raise Fourth Amendment problems. As will be discussed, whether courts adopt either version or avoid the Fourth Amendment questions altogether, the constitutional issues present an existential challenge to the future of video analytics technology.

### *A. Video Analytics as a Search—Step One: "Digital Is Different"*

This subpart sets up a two-part argument about video analytics and "reasonable expectations of privacy." Section one sets the stage, arguing that video analytics technology should not be confused with traditional video

231. Kwet, *supra* note 78 ("With city spaces blanketed in cameras, and video analytics to make sense of them, law enforcement agencies gain the capacity to record and analyze everything, all the time. This provides authorities the power to index and search a vast database of objects, behaviors, and anomalous activity.").

232. *See infra* subpart III(A).

233. *See infra* subpart III(B).

234. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against '*arbitrary* power.'" (emphasis added) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

surveillance but approached on its own terms. Section two examines the logic behind the traditional canon—finding no expectation of privacy in public—arguing that this analysis does not fit the reality of video analytics in public settings.

*1. Video Analytics Is Not Traditional Video Surveillance*.—It is easy to conflate traditional video surveillance with modern video analytics. Both appear to involve cameras, video streams, and police observation. However, any court tasked with analyzing the Fourth Amendment considerations of video-capture needs to be clear whether they are examining traditional video surveillance or AI video analytics.

For judges, the most compelling reason for this distinction is that the law governing traditional video surveillance is already well settled.[235] Challenges to traditional video surveillance cameras in public have failed for years, with a consensus emerging that most video surveillance (traditional CCTV cameras, etc.) are not Fourth Amendment searches.[236] Most persuasively, the *Carpenter* majority expressly exempted the continued use of video security cameras from its CSLI holding, leading to the inference that the Court found such traditional surveillance constitutional.[237] It is hard to

235. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 (2002) ("[A]ll courts that have considered application of the Fourth Amendment to cameras aimed at public streets or other [highly frequented] areas . . . have declared that such surveillance is not a search, on the ground that any expectation of privacy one might have in these areas is unreasonable.").

236. As discussed in Part II, case law from the 1960s through the 1990s can be read to offer little expectation of privacy in public. Whether we consider the overflight cases of *Ciraolo* or *Riley* or the beeper tracking cases of *Knotts* and *Karo*, the Supreme Court adopted the position that people lose expectations of privacy in public. *See, e.g.*, Rodriguez v. United States, 878 F. Supp. 20, 24 (S.D.N.Y. 1995) ("[A]s the activity monitored by the video surveillance occurred entirely within a public place, Rodriguez had no reasonable expectation of privacy on the public street."); State v. Augafa, 992 P.2d 723, 736 (Haw. Ct. App. 1999) ("[T]he videotaping was of a public street with unlimited access . . . . Accordingly, under the circumstances in this case, there was no objectively reasonable expectation of privacy for persons, objects, or activities which were visible to the public and hence captured by the video camera."). *But see* Montana State Fund v. Simms, 270 P.3d 64, 70 (Mont. 2012) (Nelson, J., concurring) (arguing that having fixed cameras in certain public places for security purposes is reasonable, but not "cameras that follow us all around town, monitoring and recording our every move for no purpose other than to detect and document evidence of unlawful activity" (quoting *In re* Rules of Prof. Conduct, No. OP 11-0439, at *29 (Mont. Nov. 1, 2011) (Nelson & Wheat, JJ., concurring in part and dissenting in part))).

237. *Carpenter*, 138 S. Ct. at 2220 ("We do not . . . call into question conventional surveillance techniques and tools, such as security cameras."); *see also* Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 454–55 (2018) (confirming this understanding that traditional cameras fall outside of *Carpenter*'s holding).

read *Carpenter* as altering existing law around traditional security cameras.[238]

My argument below is that just because a traditional *video surveillance* camera does not violate a reasonable expectation of privacy does not determine whether a networkwide *video analytics* system violates a reasonable expectation of privacy. Maybe it does, maybe it does not, but the reason why is not because courts unthinkingly apply the logic of one to the other.

The first step then is to distinguish video analytics from traditional video surveillance. To begin, it is important to recognize that video analytics is not doing the same thing (or collecting the same information) as what a human police officer could by watching the video screens.

Take a simple example.

At a Real-Time Crime Center *without video analytics*, a human police officer watches a man wearing a red shirt walk down Main Street. Taken alone, this observation likely falls outside of Fourth Amendment protection under a traditional canon interpretation of the law. An officer is doing what an officer could do on the street, just in the comfort of the Real-Time Crime Center. The single act is an enhancement of human visual surveillance, but not such a significant enhancement to violate an expectation of privacy under current law.[239]

Now, imagine the same image of a man in a red shirt walking down Main Street but *with video analytics* running behind the scenes. What is the analytics program doing? The analytics program is breaking down the image into classifiers—man, shirt, red shirt, pants, walking, hair color, direction, speed, time, date, etc. The analytics program saves that image within the larger dataset of every object captured by the cameras. The analytics program searches within its citywide system for similar matches of that particular red shirt and the red-shirted man (and other men wearing red shirts and all other men). The analytics program is searching to compare the object to whether it matches an anomaly trigger or unusual activity preprogrammed into the system. The dataset that is being searched is both all the collected video

238. Cases after *Carpenter* suggest there is little change to analysis about traditional video surveillance. *See, e.g.*, Commonwealth v. Mora, 150 N.E.3d 297, 307 (Mass. 2020) (recognizing that the "traditional nontargeted use of video cameras" as security cameras was "not called into question by [the] holding in *Carpenter*"); People v. Destefano, 164 N.Y.S.3d 412, 419 (N.Y. Sup. Ct. 2022) ("[The] government's use of a technology in public use, while occupying a place it is lawfully entitled to be, to observe plainly visible happenings, does not run afoul of the Fourth Amendment of the United States Constitution."); *see also* Christopher Slobogin, *supra* note 235, at 236 n.106 (listing cases).

239. While there is an open question about the aggregation of these images or when the tracking capabilities of citywide systems of video surveillance turns the act into a search, the hypothesized single act of watching a man on the street is currently not a search under Fourth Amendment law. *See supra* notes 236–238 and accompanying text.

footage from the cameras (perhaps dating back weeks or months) and the dataset of training images that allows the system to identify the particular object or action in front of the screen. The analytics program has collected data to allow it to superimpose that red shirt and compare it across time and place. The geolocational part of the program tracks the red shirt (and all red shirts) through the city. The search can be through past days or weeks and can connect the dots of the activities of all red shirts over the course of months. The analytics program does it all instantly and accurately (for the most part).[240] Inherent in the program are multiple (really, continuous) searches of past collected data, comparisons, analysis, and visualizations—all without the officer doing anything but turning on the system.

Whatever one makes of the above surveillance capacities, one thing is clear: The act is different than just watching the screen. Just because traditional *video surveillance* is not a Fourth Amendment search does not mean that *video analytics* is not a Fourth Amendment search. Video analytics should be understood on its own terms.

Note that the difference in capabilities in video analytics and video surveillance applies equally to video analytics monitoring, investigation, and anomaly detection. The description of a human police officer watching live feed of the man in the red shirt is one of monitoring and then investigation, but the same result can be seen in preprogramming a search for men in red shirts automatically. The video analytics system is digitizing every object, and that is decidedly different than what happened with ordinary analog surveillance and human observation.

Simply put, video analytics offers a different technological power than traditional video surveillance. Video analytics does more than monitor people or things in public. The system captures, sorts, stores, processes, matches, compares, tracks, and locates a person or thing over time. Whatever expectations of privacy we might have developed around one technology does not determine the outcome for a qualitatively different and quantitatively more powerful technology. Of course, recognizing the difference does not answer the ultimate Fourth Amendment question. Step one simply means that video analytics needs to be seen as a new problem without a settled answer in existing law.

*2. The Underlying Logic of "No Privacy in Public" Does Not Fit Video Analytics.*—This second section examines the logic that created the traditional "no expectation of privacy in public" principle as applied to video analytics. As mentioned, the traditional "no expectation of privacy in public" logic is built on three related arguments. First, it is argued that a person's

240. Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. 2007, 2028 (2022) (describing data and algorithmic errors in the criminal legal system).

knowing and voluntary exposure to public observation essentially forfeits a claim to privacy.[241] Second, it is argued that, because a human police officer could watch the person on the street without it violating an expectation of privacy, a camera doing the same thing does not change the expectation.[242] Third, it is argued that, in public, there is nothing private or intimate being revealed beyond what any other person could see.[243] In other words, in public, one expects to be seen by other humans, so what is being seen is not very personal, private, or intimate, and thus not protected (at least for short-term observations).

Such logic does not neatly fit video analytics. While one might know they are being observed in public, that is not the same thing as voluntarily agreeing to be classified, sorted, processed, matched, and tracked over time and place by an algorithm while in public. Those are different capabilities, and arguing that you have no expectation of privacy in public does not mean that you have no expectation of privacy against those other tracking, sorting, and storing capabilities.[244] Ask yourself whether, as you walk down Main Street, you are voluntarily and knowingly agreeing to be sorted, categorized, matched, and tracked by a police algorithm with data saved for months. Whatever your answer is, it is not controlled by the traditional canon of cases.[245]

Second, as discussed in Part II, the Fourth Amendment doctrine around expectations of privacy has been largely controlled by human

241. California v. Greenwood, 486 U.S. 35, 41 (1988) ("[T]he police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. Hence, '[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'" (quoting Katz v. United States, 389 U.S. 347, 351 (1967))); *see* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 148 (2016) (discussing knowing disclosures and the Fourth Amendment).

242. *E.g.*, Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 181 (1st Cir. 1997). Discussing the Fourth Amendment implications of cameras, the court in this case explained,

> [N]o legitimate expectation of privacy exists in objects exposed to plain view as long as the viewer's presence at the vantage point is lawful. . . . And the mere fact that the observation is accomplished by a video camera rather than the naked eye, and recorded on film rather than in a supervisor's memory, does not transmogrify a constitutionally innocent act into a constitutionally forbidden one.

*Id.*

243. *See* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 15–16 (2020) (discussing the role of "intimacy" in Fourth Amendment doctrine).

244. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1485–86 (2019) (discussing the shortcomings of consent doctrine in the digital context).

245. *See* Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 189–90 (2008) (discussing the concept of spatial privacy and how the law shapes expectations).

observations.[246] The overflight cases (*Ciraolo* and *Riley*) were both expressly limited to human observation, even though mechanical transportation was involved.[247] The beeper cases (*Knotts* and *Karo*) also turned on the limits of human tracking capabilities, even though a wireless beeper was used.[248] The Supreme Court relied on an analogy to human observations as the limiting factor for finding no reasonable expectation of privacy in public.[249] In cases where the Supreme Court protected an expectation of privacy, more than human surveillance was at issue. *Kyllo*'s protection of the home turned on technological (non-human) enhancements.[250] Cases like *Carpenter* and *Jones* which involved technological tracking powers also found an expectation of privacy in part because of the quantitatively and qualitatively different privacy harms in digital policing.[251] Video analytics offer decidedly non-human capabilities, giving police departments superhuman powers to see everything and catalog everyone.[252] Measured against expectations of privacy from human observers, video analytics is far more powerful and revealing. The system is "qualitatively different."[253] Again, while there is

246. The one exception to this rule is the Supreme Court's decision in *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), involving surveillance of an industrial plant for environmental protection investigation reasons. *Id.* at 229. In *Dow Chemical*, the Court allowed for powerful camera surveillance. *Id.* at 239. Explaining its holding, the Court stated:

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

*Id.* at 228. This holding was limited in *Kyllo*. *See* Kyllo v. United States, 533 U.S. 27, 33 (2001) ("While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical*, we noted that we found 'it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened.'" (quoting *Dow Chem. Co.*, 476 U.S. at 237 n.4)). For more discussion about *Dow Chemical*, see Ferguson, *supra* note 211, at 830–32.

247. California v. Ciraolo, 476 U.S. 207, 213 (1986); Florida v. Riley, 488 U.S. 445, 448 (1989).

248. United States v. Knotts, 460 U.S. 276, 285 (1983).

249. *Id.* at 282 ("Visual surveillance from public places . . . would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied . . . on the use of the beeper to signal the presence of Petschen's automobile . . . does not alter the situation.").

250. *Kyllo*, 533 U.S. at 34, 40 ("To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.").

251. *See supra* notes 176–194 and accompanying text.

252. Ferguson, *supra* note 171, at 31–32 ("Superpowers that offer police the ability to circumvent natural human privacy barriers are considered searches (like seeing and hearing through walls), whereas technological enhancements of human senses (flashlights and telescopes) fall outside of Fourth Amendment search scrutiny.").

253. This is the term from *Riley* and *Carpenter*. Riley v. California, 573 U.S. 373, 395 (2014); Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

nothing in the doctrine that explicitly states expectations of privacy are limited by what humans can see without technological assistance, the traditional canon does suggest that distinction.

Third, there is what might be called the "nothing private in public" logic that nothing personal or intimate is being revealed in public spaces. Underlying the diminution of privacy is the claim that nothing personal is being uncovered by police observation. This argument is contestable as a factual matter, as a person's public presence outside an abortion clinic, chemotherapy center, or psychologist's office might be quite revealing of personal matters. The logic is also strained if police are watching for long periods of time (episodically or continually), since the Supreme Court held long-term tracking to be a violation of an expectation of privacy because it revealed too many of the privacies of life.[254]

Yet, this third point does raise some complexities. For example, if all one imagines is a short-term use of video analytics on a virtual patrol that does not reveal intimate, personal details, then there may be some truth to this argument. Limited monitoring akin to a human watching the same video feed tracks the traditional logic of no expectation of privacy in public. The problem is that this hypothetical is an artificial, if not misleading, account of what is happening with video analytics technology. Just because the human officer is merely using the surveillance cameras for a particular virtual patrol, that does not mean that the pattern matching system is not running and categorizing everything in the camera's path behind the screen. In addition, the "short-term" categorization is inexact, as the objects are saved and searchable for weeks or months by default. If every object is being identified and tracked in the video frame, it is not accurate to artificially focus on just the point in time the officer is paying attention. The privacy harms are systemic, not episodic.[255]

If you have just read the above paragraphs and concluded that video analytics is a bit more complicated than you thought, and you are unsure of how you feel about AI-powered computers pattern matching you as you go about your life, you might have also answered the reasonable expectation of privacy question under the traditional canon. It just is not settled. Objectively, we do not expect (and most of us do not even know) that computer vision is performing object-recognition pattern matching on our lives, and thus, expecting so would be unreasonable. It would seem a stretch to claim that you objectively and reasonably expect (or have voluntarily agreed) that your

254. *See supra* notes 181–182 (discussing *Carpenter* and the *Jones* concurrences).

255. In a prior article, I address how similar systems of surveillance, such as the persistent surveillance planes like those that flew over Baltimore and long-term pole cameras, create similar systemic harms. Ferguson, *supra* note 171, at 48.

pixels will be identified in a network of cameras stretched across a city and that society thinks such an expectation is reasonable.[256]

Applying the traditional canon to the problem of video analytics is ultimately unsatisfying. Expectations are different. Surveillance capabilities are different. The logic of public exposure does not fit systems of continuous surveillance. At a minimum, this argument shows that courts must keep an open mind about video analytics and not blindly apply old-fashioned video surveillance precedent to a very different privacy problem.

### *B. Video Analytics as a Search—Step Two: AI-Enhanced Is Different*

To say that traditional Fourth Amendment doctrine does not resolve modern technological puzzles is not unusual. Video analytics, like similar digital tracking technologies (e.g., facial recognition or smart city sensors), raise hard constitutional questions as new technologies and old laws intersect.[257] The first step of my argument merely posits that courts should not unthinkingly apply old precedent to a new problem, because the technology and privacy issues are just too different.[258]

The second step of my argument goes further, explaining that automated, AI-enhanced video analytics is a Fourth Amendment search violating a reasonable expectation of privacy. Further, use of video analytics is likely an unconstitutional search because no warrant can be obtained before the generalized pattern matching occurs in a system of continuous surveillance.[259] Whether we are talking about investigation, virtual patrols, or anomaly alerts, the citywide object-recognition process occurs, and must occur, before any particularized suspicion attaches. Video analytics surveillance is, by design, a general search, and violative of societal expectations of privacy.

This second step of my argument builds upon the logic of the new "digital is different" cases to show that video analytics is more privacy invasive than GPS or CSLI tracking, and the privacy harm cannot be mitigated with a warrant. Again, at least in cities with hundreds or thousands of networked cameras, this exposure violates a reasonable expectation of privacy, and thus the Fourth Amendment.

---

256. The en banc court in *Leaders of a Beautiful Struggle v. Baltimore* identified a similar harm with the potential identification of any person using the persistent surveillance system planes. 2 F.4th 330, 333 (4th Cir. 2021).

257. *See* Ferguson, *supra* note 80, at 1127–28 (discussing facial recognition); Ferguson, *supra* note 35, at 51–52 (discussing smart cities).

258. *See* Ferguson, *supra* note 211, at 853 (detailing how archaic many of the technologies were that still serve as precedent in modern cases).

259. *See infra* subpart III(C).

*1. The Logic of Mass Digital Surveillance*.—The Supreme Court's recent digital surveillance cases offer two clues to show how expectations of privacy have changed in the face of systems of mass surveillance like CSLI or GPS tracking. First, *Carpenter* and *Jones* explicitly protect geolocational privacy from digital tracking—even in public.[260] Second, those cases highlight a concern with systems of data collection that are arbitrary, aggregating, permeating, and allow overbroad retrospective queries.[261] At some moment along a (still unsettled) continuum, the Supreme Court has found police surveillance powers to violate a reasonable expectation of privacy.[262] Doctrinal clues about both (1) tracking movements in public and (2) surveillance systems are helpful to answer the video analytics search question. Both point toward the claim that a police surveillance power like AI-powered video analytics in a Real-Time Crime Center violates the reasonable expectation of privacy of a suspect caught by the cameras.

*a. Tracking Movements in Public*.—After *Carpenter* and *Jones*, it can no longer be said that people automatically forfeit an expectation of privacy in public. At core, *Carpenter* and *Jones* both suggest a concern with the revealing nature of tracking data—even in public spaces.[263] The defendants in *Carpenter* and *Jones* were moving in public, and yet they did not forfeit an expectation of privacy simply because they were exposed. Antoine Jones was driving on public streets in a publicly observable Jeep Cherokee for almost a month.[264] Timothy Carpenter was tracked from store to store by his cellphone location.[265] In keeping with the *Katz* principle that one can still maintain some privacy in public, the Supreme Court has twice protected public location data.

Justice Alito's concurrence in *Jones* specifically acknowledged all the methods by which Jones could have been tracked in public without violating the Fourth Amendment, but also conceded that long-term digital tracking, even in public, ran afoul of the Fourth Amendment.[266] The *Carpenter* Court could have analogized to *Knotts* to argue that Timothy Carpenter had

260. Carpenter v. United States, 138 S. Ct. 2206, 2218–19 (2018) (discussing the "tracking capacity" of CSLI); United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (discussing tracking as a search).

261. Ferguson, *supra* note 80, at 1129–41 (discussing these principles as part of how the Court can "future-proof" the Fourth Amendment).

262. *See* Ferguson, *supra* note 35, at 80 (describing a similar continuum analysis).

263. *See infra* note 269 and accompanying text.

264. *Jones*, 565 U.S. at 403.

265. *Carpenter*, 138 S. Ct. at 2212–13.

266. *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in the judgment) ("The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.").

knowingly exposed his location by being in public.[267] The Court also could have analogized to *Miller* or *Smith* (the third-party records cases) to argue that Carpenter had voluntarily revealed his location data to a third party cellphone provider.[268] Instead, the Court found (long-term) location data to be constitutionally protected because society does not expect to be publicly tracked by the police in this manner.

Video analytics through Real-Time Crime Centers offers a more revealing digital tracking power than either GPS or CSLI. With video analytics, police get not only location and time but also content of what the person is doing in public. Whereas with GPS and CSLI, police need to infer activity from the location, with digital video analytics, police see the activity on video. One must assume that if police also had used video analytics to follow *Jones* and *Carpenter* around town in addition to GPS or CSLI, it would have been easier for the Supreme Court to find a violation of an expectation of privacy.

The long-term nature of the tracking was important. *Carpenter* and *Jones* limited their holdings to the problem of long-term tracking, now understood as the collection of more than seven days of information.[269] Such collection is within the default collection times for video analytics systems, as the systems are programmed to collect and save information for weeks or months.[270]

Before moving on, this last point about the scale and scope of tracking data should be emphasized. It is easy to see how video analytics *investigation* creates a parallel to a *Carpenter–Jones* search analysis of long-term tracking in public through collected data.[271] With an appropriate search query, police can locate a Jeep Cherokee in the camera data over the last days, weeks, etc. Like CSLI, object location (car or person) can be mapped over time. Whether it is seven days or twenty-eight days, the locational exposure that concerned the Court in *Jones* and *Carpenter* is the same (or likely even more revealing with video analytics).

But note that even if the officers are merely passively observing the video on a virtual patrol, or if an anomaly alert has been preprogrammed into

267. Justice Kennedy makes this exact point in dissent, arguing *Knotts* held the opposite of what the majority in *Carpenter* used it for. *Carpenter*, 138 S. Ct. at 2231 (Kennedy, J., dissenting).

268. *See id.* (Kennedy, J., dissenting) ("The Court continues its analysis by misinterpreting *Miller* and *Smith*, and then it reaches the wrong outcome on these facts even under its flawed standard.").

269. *Carpenter*, 138 S. Ct. at 2217 n.3 (determining that seven days of historical CSLI was a search); *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (raising concern about a "comprehensive record of a person's public movements that reflects a wealth of [personal] detail"); *id.* at 424, 429–30 (Alito, J., concurring in the judgment) (mentioning "long-term tracking").

270. *See* Larkman, *supra* note 1 (discussing data retention practices).

271. Both *Carpenter* and *Jones* were cases involving tracking technology to retrospectively search through location data.

the system, the analytics program is still automatically tracking movements and identifying everyone in public for long periods of time behind the scenes. Just because a police officer is not actively sorting through the data does not mean that law enforcement systems are not collecting and cataloging the data about particular people doing things in public. The only reason why the investigative query works is because all the visual objects have already been collected, matched, and tracked by the system as they appear. Whether passive, preprogrammed, or for investigative purposes, the video analytics program is continuously pattern-matching objects (and people) in time, space, and location.

This reality is the key technological strength and the central constitutional flaw with video analytics: By design, video analytics in a Real-Time Crime Center is constantly searching in a generalized and overbroad manner. Whether the police officer actively queries the system, passively watches it, or lets a preprogrammed algorithm search, the same object-recognition matching process is running on the system. This AI-enhanced, technological reality complicates the constitutional analysis, because while intuitively it might seem like certain police actions (e.g., human-initiated, active, long-term retrospective queries of stored datasets) are more violative of expectations of privacy, the same pattern-matching and tracking process is happening passively and automatically behind the scenes in the ordinary course of use. Put another way, if the police department designs a video analytics program to capture, identify, and automatically match every object in public, they cannot claim they are not tracking everything in public just because a particular police officer chose to focus on one point in time.

*b. Systems of Surveillance*.—The second clue from *Carpenter* and *Jones* is that the Supreme Court shifted its concern to systems of mass surveillance. The privacy harm articulated by the Supreme Court in both cases focused on the need to control governmental *surveillance systems* that were arbitrary, permeating, aggregating, and provided a retrospective search capability. As detailed in the cases, both CSLI and GPS technologies created vast datasets of personal information that allowed police an almost limitless power to observe individuals across time and space. If collecting and searching through the data was not a Fourth Amendment "search," then police would have the power to watch anyone for any reason, using the data trails left behind.[272] In addition, both GPS and CSLI technologies allowed police to aggregate different data points with other information, revealing personal

272. Imagine that *Jones* had come out the other way. It would have allowed police to obtain a GPS dataset of all cars that police tagged without a warrant. It would also have allowed police the ability to watch John Roberts' car at will, tracking it across time and space without a warrant.

details about a life.[273] Watching an individual can reveal health concerns, political interests, dating preferences, and other habits and hobbies. While not explicit in their opinions, the Justices appeared to be concerned with chilling associational freedoms[274] and revealing "the privacies of life."[275] Combining these concerns together, the Supreme Court drew the line at digital systems of surveillance that were too permeating and arbitrary and that allowed for comprehensive, retrospective, and aggregating details of personal lives and associational connections.[276] In other words, a system of surveillance that could reveal these privacies of lives was one that violated a reasonable expectation of privacy.

The hard part for courts, of course, is identifying which systems of surveillance violate the Fourth Amendment and which do not. In a series of articles, I have developed a "future-proofing" framework to examine systems of surveillance.[277] My Fourth Amendment framework shows how the Supreme Court has drawn the line against certain threats posed by digital surveillance systems.[278] The framework distills seven factors from the "digital is different" cases to test which systems of digital surveillance should be considered a violation of a reasonable expectation of privacy, and thus a Fourth Amendment search.

The future-proofing framework reveals how certain types of surveillance systems, like video analytics, raise Fourth Amendment privacy concerns. First, as discussed, the systems are *tracking* technologies that

273. Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579 (2017) ("[W]hen database queries about particular U.S. persons have the capacity to aggregate data such that it will reveal information that, in the absence of aggregation, the government could only access by conducting a search or seizure, the extraction of that information should be subject to constitutionally based limits.").

274. *See infra* note 284 and accompanying text.

275. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

276. Scholars have interpreted *Carpenter* in different ways, offering different conclusions about the factors that might be determinative in finding a search in the face of new surveillance technologies. *See, e.g.*, Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1801–04 (2022) (examining factors including the revealing nature, amount, number of people affected, inescapability, automatic disclosure, and cost); Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 13 (2020) (describing three emerging factors, including "the intimacy of the place or thing targeted . . . the amount of information sought[,] and the cost of investigation"); Paul Ohm, *supra* note 194, at 361 (gleaning critical factors from a "close reading" of the opinion).

277. *See* Ferguson, *supra* note 80, at 1132–40 (detailing the "future-proofing" principles); Ferguson, *supra* note 35, at 53 (developing this analysis); Ferguson, *supra* note 171, at 45–46 (same).

278. Ferguson, *supra* note 80, at 1129; Ferguson, *supra* note 35, at 74–75; Ferguson, *supra* note 171, at 54.

reveal movements and patterns in physical space.[279] Second, the technologies are *too permeating* in nature, making data capture difficult to avoid.[280] Third, the technologies are *arbitrary* and broadly applicable, with no judicial limitations on what data is collected or whether the search can be applied against everyone.[281] Fourth, the data collected is *retrospectively* searchable, allowing for indiscriminate and indeterminate searches into the information.[282] Fifth, the collected data can be *aggregated* to reveal personal details, patterns, or hidden connections that would not be connectable otherwise.[283] Sixth, the impact of these technologies undermines *associational freedoms*, religious activity, dissent, personal choice, and infringes other constitutional rights.[284] Finally, the technologies provide a qualitatively different *superpower* that makes the technology more than a

279. *See supra* note 271 and accompanying text (discussing tracking); Chokshi, *supra* note 122 ("Software is also being trained to identify a wide range of activities, such as using a phone, shaking hands, punching something, drinking beer and walking toward or away from an object.").

280. *See Carpenter*, 138 S. Ct. at 2214 ("[A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

281. A concern with arbitrary policing power is central to Fourth Amendment theory. *See id.* at 2213 ("The 'basic purpose of [the Fourth] Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against *arbitrary* invasions by governmental officials.'" (emphasis added) (quoting Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 528 (1967))); *see also id.* at 2213–14 ("Although no single rubric definitively resolves which expectations of privacy are entitled to protection, . . . our cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against '*arbitrary* power.'" (emphasis added) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))); *see also, e.g.*, United States v. Ortiz, 422 U.S. 891, 895 (1975) ("[T]he central concern of the Fourth Amendment is to protect liberty and privacy from arbitrary and oppressive interference by government officials."); Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 309 (1998) ("The Fourth Amendment was a creature of the eighteenth century's strong concern for the protection of real and personal property rights against arbitrary and general searches and seizures.").

282. As the Supreme Court stated in *Carpenter*:

> [T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years.

*Carpenter*, 138 S. Ct. at 2218; *see also* Stephen E. Henderson, *supra* note 118, at 947–48 (discussing the danger of giving police a "time machine" to go back to investigate anything they wish).

283. Both *Jones* and *Carpenter* discuss the privacy harms from aggregating different pieces of personal data. United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring); *id.* at 429–31 (Alito, J., concurring in the judgment); *see also* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1834–35 (2014) (describing the mosaic theory and its privacy harms).

284. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

human enhancement from an analog era.[285] Each of these factors is contestable, but over the course of three previous articles, I have shown how they reveal the core rationale of the "digital is different" surveillance cases.[286] At a minimum, the framework offers a way to re-envision video analytics in Real-Time Crime Centers and see the systemic privacy issues at stake.

*i. Future Proofing and Video Analytics Investigation*.—Video analytics *investigation* offers the clearest parallel to what happened in *Carpenter* and *Jones*. One can easily imagine police officers using object recognition to find Jones' Jeep on city streets or Timothy Carpenter (in pixels) as he walked in and out of various electronics stores. As with GPS and CSLI, police can use video analytics in a Real-Time Crime Center to trace objects and people across the city.[287]

Applying the future-proofing framework to the question of video analytics investigation suggests such queries are Fourth Amendment searches. Beyond the fact that the officer literally is searching a video database for information about suspects, the nature of the surveillance is similar to acquiring CSLI records and accumulated GPS data, which the Supreme Court has deemed a violation of an expectation of privacy.[288]

Specifically, with video analytics investigation, a police officer can *track* an individual or object from place to place across time. The camera systems are *permeating*, allowing police to see every connecting point the camera scans in a city. The lack of judicial oversight means that the search can be *arbitrary*—allowing police to follow suspects, witnesses, or even politicians and ex-girlfriends without any laws or judicial authorization regulating use. The searches are *retrospective*, allowing objects to be identified from past data over weeks or months. The details from the searches are even more revealing than cell-site location because, as mentioned, in addition to location, you can visually observe what someone is doing.[289] The cameras reveal not just place but activity, and those details can be *aggregated* with other information to discover patterns in a life. *Associational* connections can be observed from the video streams. This information can be used not only to identify criminal associates but also to investigate First

285. Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the* Carpenter *Decision*, 16 OHIO STATE J. CRIM. L. 281, 287 (2018) ("[T]he new technologies of policing employ data collection, storage, and analysis methods that are both *superhuman and cheap*. They are superhuman because while human beings could do the same thing, it would be impracticable to do so.").

286. *See generally* Ferguson, *Persistent Surveillance*, *supra* note 171; Ferguson, *Facial Recognition and the Fourth Amendment*, *supra* note 80; Ferguson, *Structural Sensor Surveillance*, *supra* note 35.

287. *See supra* notes 118–120 and accompanying text.

288. *See supra* notes 178–194 and accompanying text.

289. *See supra* subsection III(B)(1)(a).

Amendment protected activities in public or to reveal intimate partners and lifestyle choices. Again, if a searchable system of location data (CSLI/GPS) reveals enough to violate a reasonable expectation of privacy, then a searchable system of location data *plus video images* must also violate a reasonable expectation of privacy and be considered a Fourth Amendment search.

*ii. Future Proofing and Video Analytics Monitoring*.—If the above argument persuades you that video analytics *investigation* is a Fourth Amendment search, remember that the technology of video analytics *monitoring* is essentially the same. The only difference is what initiates the query, not what is happening behind the scenes as a technological matter. Whether the officer goes back in time to find an object, or whether the technology identifies the object on its own, the same retrospective pattern matching is occurring. Inherent in the AI system of pattern matching is the continuous process of retrospective searching and matching so that an object can be identified in real time.

Applying the future-proofing framework to virtual patrols, police are using a system of cameras that is *permeating* such that it can watch individuals as they go about their lives. Without judicial restrictions, any virtual patrol will be *arbitrary*, left to the discretion or curiosity of an officer. Activities and *associational* connections can be flagged and, over time, *aggregated* to reveal insights about the privacies of life. The main distinction from investigation is that the retrospective nature of the *tracking* is lacking.

However, even if the temporal element is missing (i.e., assume that there was no retrospective searching back in time), there is still a parallel privacy harm to CSLI and *Carpenter*. After all, one might imagine that if police were just skimming through the CSLI data of everyone in America to see what they were up to—essentially a virtual CSLI patrol—the Supreme Court would find such arbitrary action a Fourth Amendment problem. This is the reality of video analytics in a city with a sophisticated camera network. Object recognition code is just scanning the collected video data to observe, connect the dots, and conduct virtual patrols. All the concerns of an arbitrary, pervasive, tracking system exist, except the harm runs to everyone in the system. The suspect and everyone else are being monitored by a visual object tracking system.

*iii. Video Analytics and Anomaly Alerts*.—Anomaly alerts present a different privacy question than video analytics investigation or monitoring. While the object recognition technology behind anomaly alerts is the same as the technology powering investigation and monitoring, there are different privacy impacts in application.

For example, if a computer alerts to the presence of an individual in a parking lot when there is ordinarily no movement in the parking lot, can that person have any claim to an expectation of privacy in public when the algorithm alerts to the act? Is the police algorithm "searching" when it alerts to a match for a preprogrammed anomalous movement or object?

As a practical matter, there are differences that make anomaly alerts less privacy invasive than investigation or monitoring. First, the focus of suspicion is a place or an unusual action and not directed at a person. An alert, which was preprogrammed, for movement in a park at night is suspicious because of the location, not necessarily the person. Second, the amount of information revealed is far less than in the investigation situation. The object recognition will alert to what is happening in the park, but not necessarily aggregate that data with other information. Relatedly, the temporal aspect is less extensive, as the alert focuses on a particular time and does not include other information about other times. Finally, the preprogrammed nature of the suspicion seems less arbitrary and pervasive, as it has been preplanned and is essentially suspicionless.[290] The result is that there is both less private information revealed, or even potentially revealed, and less concern about police discretion and abuses in an anomaly alert.[291]

Applying the future-proofing principles to anomaly alerts confirms these different privacy impacts. For example, anomaly alerts (e.g., bag detection, unusual movements) are not primarily *tracking* technologies. They identify movement in time, not paths or patterns along a timeline. Second, while the surveillance is *permeating* in that the cameras and alerts are everywhere, the anomaly, by definition, is an unusual event. Anomalies are not continuous but involve episodic surveillance. Because the alerts must be preprogrammed, they are less arbitrary, as the preset criteria have been designed in advance, reducing the discretion of individual officers. In addition, the preprogrammed nature of the alert distinguishes the alert from retrospective searches into past data and makes *aggregation* of personal data

290. *See* Christopher Slobogin, *Suspectless Searches*, 83 OHIO ST. L.J. 953, 958 (2022) (discussing how suspicionless searches require a different Fourth Amendment analysis).

291. There are other reasons to object to anomaly detection outside the Fourth Amendment context. *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1990, 1995, 2008 (2017) (discussing propensity to error and display bias in algorithmic and other machines utilized in legal processes). Predictive suspicion systems raise real concerns with error, bias, and equity (in investigation and at trial). The preprogrammed suspicion prompts are developed outside the policing context by private developers, and might not take into account issues of economic, social, or racial differences. *See* Eric Lander & Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED (Oct. 8, 2021, 8:00 AM), https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/ [https://perma.cc/45K7-43PA] (discussing how algorithms may inadvertently import the biases of the training sets they use); Zewe, *supra* note 46. In addition, it is difficult to determine *ex ante* what is going to be deemed "suspicious" in the future. Almost all data driven testimony suffers from this inherent bias that confuses technology with objectivity. Roth, *supra*, at 2007.

difficult. Of course, these systems can still chill *associational* freedoms[292] and do offer a *superpower* beyond any human capability, but the privacy impacts are different.[293]

Even acknowledging the difference with anomaly alerts, however, we run into a now-familiar problem. To work as designed, the cameras must always be searching for what they have been programmed to find and thus seeing everything else. This point—that to work, the system must always be on and searching—raises a bigger question that must be addressed by courts trying to think through the Fourth Amendment questions around anomaly alerts.

Here is the problem restated: Should courts focus on the system that surveils or just the result of the surveillance? If a court focuses on *the system* that allows for anomaly detection, it will see a system that potentially reveals location, aggregates information, allows retrospective searches, and offers a permeating and arbitrary form of surveillance. The anomaly alert may only be programmed for one thing, but the system must catch it all to see the anomaly. On the other hand, if a court focuses on the result of the automated alert that is obtained—an alert about an individual who is flagged doing something unusual—the privacy harm seems less significant.[294] The question for judges is which one is the proper focus.

In prior work, I have called this distinction "the unit of surveillance" question,[295] and it likely would shape the Fourth Amendment answer to anomaly alerts. The unit of surveillance is a framing mechanism. If you zoom out to see the systems working to collect information, you see a privacy threat that aligns with what the Supreme Court articulated in *Carpenter*, *Jones*, and *Riley*.[296] If you zoom in and just look at the particular information collected, the privacy harm is less obvious. The unit of analysis matters.

In *Carpenter*, for example, the Supreme Court chose to focus on the systems of collection rather than the actual information being collected, suggesting that the Court cared more about the potential investigatory power of CSLI than the actual use of that power.[297] The Court explicitly warned

292. For example, if the anomaly algorithm were set to identify people attending a meeting of an anarchist group or any organization committed to dissent against the government, such an alert would chill associational freedom. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

293. Joh, *supra* note 285, at 287.

294. This question about focus is almost never asked or even acknowledged in Fourth Amendment cases. Yet, it helps resolve how courts decide the issues. The "digital is different" cases focus on the systemic nature of collection. *See infra* notes 300–303 and accompanying text. The traditional canon cases focused on the result of that collection.

295. Ferguson, *supra* note 171, at 4 (discussing the term).

296. *See infra* notes 300–303 and accompanying text.

297. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (focusing the Fourth Amendment analysis on the CSLI system of collection).

about a power that could uncover data about anyone for any reason.[298] The Court deemphasized the revealing nature of the actual data collected—after all, the fact that Timothy Carpenter was in a few stores at the relevant time of the robberies is incriminating but not revealing of privacy interests.[299] Instead, the harm the Court focused on was the potential reveal that such a system of data collection (400 million phones) could expose more broadly.[300] The same analysis can be applied to the *Jones* concurring opinions, which identified the harm as the potential chilling impacts of tracking everyone without a warrant, not the privacy harm of whether Antoine Jones was near a particular narcotics stash house or not.[301]

In other words, if the unit of surveillance to be studied is *the system* of mass data collection, there is a Fourth Amendment concern with anomaly alerts in the video analytics system. To find the anomaly, the system must be searching everything captured in its cameras. If the unit of surveillance to be analyzed is just the information obtained, perhaps there is less privacy harm.

All the above discussion suggests that video analytics—in all its forms—raises concerns similar to CSLI and GPS surveillance and likely should be considered a Fourth Amendment search. The "video analytics as a search" argument would consider all forms of video analytics in citywide Real-Time Crime Centers a violation of a reasonable expectation of privacy and unconstitutional absent a warrant or exception. Police can still watch camera systems without video analytics enabled, but turning the cameras into digital tracking systems via AI pattern-matching technology creates Fourth Amendment privacy harms.

*2. Warrants and Video Analytics Systems.*—*Carpenter* and *Jones* did not declare police acquisition of GPS or CSLI data unconstitutional; the Supreme Court merely required a judicial warrant to obtain the information.[302] The same logic should hold for police wanting to query video analytics data. If the use of video analytics is a Fourth Amendment search, then a warrant (or

298. *Id.* at 2218 ("[B]ecause location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

299. *Id.* at 2218, 2220.

300. *Id.* at 2218.

301. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government . . . chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring))); *id.* at 403–04 (majority opinion).

302. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2221 ("[T]he Government's obligation is a familiar one—get a warrant.").

exception) is required.[303] In practical terms, to find the robbery suspect in the red shirt from the collected video streams digitally sorted by object across a city, police must first obtain a warrant.

But here is the problem. Police cannot get a warrant *before* the video analytics system has captured all the objects and patterned matched them. True, police can get a warrant to find the robber in a red shirt at a particular place and time *after* the citywide collection, but to locate that particular red shirt, police already had to have collected images of everyone wearing a red shirt.[304] By design, computer vision has been finding red shirts in the city (along with every other color shirt) all along. The collection of information about everyone, everywhere has already happened—all without a warrant. Simply put, the unconstitutional collection has already occurred before a warrant can be obtained for a particularized use.[305]

To go back to the *Jones* case, the analogous situation would be if police had placed GPS devices on all private cars to collect location data on all drivers.[306] Or, in *Carpenter*, if law enforcement had directly collected all CSLI signals (as opposed to a private company) on all cell phone users in order to track location.[307] In both cases, the question would not be whether a warrant could be obtained but whether this initial act—independent of the later warrant—would have violated the Fourth Amendment. Both *Jones* and *Carpenter* suggest that these acts would violate a reasonable expectation of privacy.[308] To be fair, these were not the factual circumstances in *Jones* or

303. Similar reasoning has been debated in appellate court decisions that have addressed analogous surveillance questions. For example, the Fourth Circuit Court of Appeals considered a challenge to an aerial surveillance plane that was able to capture video of the entire city of Baltimore over twelve-hour time periods. The question presented in *Leaders of a Beautiful Struggle v. Baltimore* was whether this form of surveillance was a search. 2 F.4th 330, 333 (4th Cir. 2021). The en banc court concluded that such systemic citywide surveillance violated a reasonable expectation of privacy and was a search for Fourth Amendment purposes. *Id.*

304. Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 GEO. MASON L. REV. 412, 413 (2018) (describing the tension of how the Fourth Amendment addresses collection and not use).

305. The debate about Fourth Amendment collection and use restrictions has been an ongoing one. *See* Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 138 (2018) (discussing the contrast between use and collection restrictions); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 6 (2015) (identifying two stages of digital evidence collection: the physical search for the devices themselves and the electronic search of the data on the devices).

306. In fact, during oral argument in *Jones*, Chief Justice Roberts asked the Deputy Solicitor General whether the government's position was that they could put a GPS device on the Justices' cars. Transcript of Oral Argument at 9, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259).

307. *See Carpenter*, 138 S. Ct. at 2223 (declining to "call into doubt warrantless access to CSLI in . . . an ongoing emergency").

308. One need not imagine too much, because police have contracted with a company called Fog Data Science, which runs a search engine called Fog Reveal, that provides geolocational data to police as a paid service. To work as a retrospective search, the system must collect and retain the

*Carpenter*, but GPS tracking of all cars and government-CSLI tracking of all phones are more privacy invasive than the facts of those cases. As with video analytics, a judicial warrant would not cure the harm of overcollection and suspicionless rummaging because the harm is in collecting the data in the first instance.[309]

Similarly, and perhaps more intuitively, police cannot obtain a warrant for video analytics-enhanced virtual patrols before the patrol. As a practical matter, getting a warrant to allow police to monitor video cameras in real-time makes little sense. The whole point of a virtual patrol is to allow the AI system to skim across the camera feeds looking for suspicious behavior, monitoring people, and scanning the streets for objects. Almost by definition, there is nothing suspicious until the pattern-matching system sees something suspicious. Virtual patrols are not particularized and are lacking in probable cause. Thus, a warrant requiring both probable cause and particularity before using the monitoring technology would not be feasible.[310]

Finally, an anomaly alert is an odd fit for a warrant requirement. The preprogrammed suspicion or identification is not individualized as the predictive code was written months or years before the alert. In addition, there is no easy way to interpose a warrant—even an anticipatory warrant—before the alert sounds.[311] The system is by design matching in a continuous and automatic fashion without the opportunity to get judicial approval for anything *ex ante*. Warrants, thus, cannot play their traditional role of assuring

locational data, thus creating precisely the concern here. Dell Cameron, *What Is 'Fog Reveal,' The Police App Tracking Your Phone*, GIZMODO (Sept. 9, 2022), https://gizmodo.com/what-is-fog-reveal-police-app-tracking-your-phone-1849514556 [https://perma.cc/YQB8-R29D]; Will Greenberg, *Fog Revealed: A Guided Tour of How Cops Can Browse your Location Data*, EFF (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-revealed-guided-tour-how-cops-can-browse-your-location-data [https://perma.cc/AS3N-WSEV].

309. Andrew Guthrie Ferguson, *Digital Rummaging*, 101 WASH. U. L. REV. 1473, 1476 (2024).

310. *See* U.S. CONST. amend. IV ("[A]nd no warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized.").

311. United States v. Grubbs, 547 U.S. 90, 96–97 (2006). According to the Court, valid anticipatory warrants require:

> [T]he magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed. It should be noted, however, that where the anticipatory warrant places a condition (other than the mere passage of time) upon its execution, the first of these determinations goes not merely to what will probably be found *if* the condition is met. (If that were the extent of the probability determination, an anticipatory warrant could be issued for every house in the country, authorizing search and seizure *if* contraband should be delivered—though for any single location there is no likelihood that contraband will be delivered.

*Id.*; *see also Fourth Amendment—Anticipatory Warrants*, 120 HARV. L. REV. 154, 154, 159 (2006) (describing the limited nature of anticipatory warrants).

particularized use of police power based on individualized probable cause.[312] The nature of continuous surveillance thwarts the normal role of the warrant requirement.

### *C. Two Views on Avoiding the Search Question*

Before concluding, it is worth considering whether courts might try to avoid the Fourth Amendment search issue altogether. Courts could choose to analyze the problem outside the somewhat ill-fitting "reasonable expectation of privacy" threshold search test. Or, courts could focus on the "reasonableness" of the police action, treating video analytics as a non-investigatory police tactic akin to a special needs search.[313] Both attempts at judicial avoidance deserve scrutiny, even if neither satisfactorily resolves the question.

*1. Avoiding the Search Question.*—One way courts could avoid the Fourth Amendment search question is to say police are not involved in the search process because all the decisions are governed by preprogrammed algorithms. Just as a matter of doctrinal fit, the timing of when the "search" was programmed and the automatic nature of the pattern matching do not take the question out of the usual human police officer situation (and the usual fear of human police officer discretion).[314]

First, as to the preprogramming argument: Preprogramming pattern-matching algorithms should not be a way to avoid Fourth Amendment restraints. While it is true that the programming and system design happened earlier in time (and by computer programmers, not police), the resulting information exposed is the same. It would be no less of a constitutional violation if police preprogrammed a computer program to hack my Wi-Fi and read the notes in my computer than if they did it in real time. In both, police are involved in the information collection process and cannot avoid constitutional scrutiny by simply preprogramming the intrusion for some time in the future.[315] Similarly, it seems appropriate to hold police to account

312. *See* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized . . . prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

313. Police must ultimately be responsible for the choices they make to buy certain technologies. For discussions on police procurement of surveillance technology, see generally Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016) and Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19 (2017).

314. *See* Slobogin, *supra* note 290, at 958 (discussing searches that are more administrative in nature).

315. *See supra* notes 213–219 and accompanying text.

for the algorithmic systems they buy and deploy in cities.[316] Police algorithms are not separate from police departments, and there is no independent non-law enforcement role of the algorithm itself deployed on police systems. It is a police tool like a thermal imager, drone, or taser, with no independent agency outside of how police use it.[317]

In addition, courts should recognize the cost in exempting algorithms from constitutional scrutiny. If the Fourth Amendment has nothing to say about video analytics in Real-Time Crime Centers, then police would be able to greatly expand sensor-driven surveillance without constitutional limits just by automating the surveillance. With no constitutional limits, police could program in the pixelated profiles of Supreme Court Justices (or at least their faces and license plates) and watch them "alert" as they traveled through the city. Each alert—if examined in isolation—might not reveal much, but in total, the constant object monitoring could be as revealing as *Jones*'s GPS data or *Carpenter*'s CSLI records.[318] Put another way, the preprogrammed and automated nature of the alert does not remove the invasion of privacy, even if isolated or targeted. If the system was preprogrammed automatically to alert to a Justice's license plate, the time it captured the car outside the chemotherapy infusion center would be privacy-invasive. Or if a preprogrammed alert sounded for every time a Justice visited the home of a wealthy benefactor, it might reveal an associational connection that deserved privacy. The fact that algorithms are doing an investigating officer's work does not change the privacy problem.

A second way to avoid the search question is that courts could analogize to established Fourth Amendment exceptions, seeing video analytics through a community caretaking lens[319] (more focused on public safety than traditional law enforcement). Doctrines like the "community caretaker" exception do allow police to search for non-criminal purposes, but

316. *See* Renata M. O'Donnell, Note, *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, 94 N.Y.U. L. REV. 544, 576–77 (2019) (arguing that police should be held responsible for algorithms that create racial disparities in violation of the Fourteenth Amendment).

317. For an interesting history of the technological tools behind early Fourth Amendment cases and the history of police tools like tasers, see generally CYRUS FARIVAR, HABEAS DATA: PRIVACY VS. THE RISE OF SURVEILLANCE TECH (2018) and MATT STROUD, THIN BLUE LIE: THE FAILURE OF HIGH-TECH POLICING (2019).

318. *See supra* notes 222, 224.

319. The Supreme Court has, on occasion, recognized that police act in a public safety/first responder capacity and thus not in a traditional investigatory role. For example, in *Brigham City v. Stuart*, the Court found entry into a house to prevent injury from a fight to be reasonable. 547 U.S. 398, 400 (2006). What had been known as the "community caretaker" exception from *Cady v. Dombrowski* has recently been narrowed in *Caniglia v. Strom*, in which the Court limited non-emergency warrantless entries in a home on a community caretaking theory. *Cady*, 413 U.S. 433, 447–48 (1973); *Caniglia*, 141 S. Ct. 1596, 1598 (2021).

establishing a citywide surveillance system to care for a city seems an expansion beyond the narrowly crafted warrant exception.

The problem with the community caretaker argument is twofold. First, police in Real-Time *Crime* Centers are searching for crime and people engaged in criminal activity. While some of the centralized operation centers were originally set up for emergency response purposes, it is hard to argue that a crime center is not trying to investigate crime.[320]

In addition, the argument that the alerts are not criminal in nature and thus outside Fourth Amendment protection has the privacy principles backwards. The idea that police can surveil more of a person's lived experience because they are not searching for a crime and do not have individualized suspicion inverts established constitutional protections.[321] It should be the case that police have to reach a higher standard to invade more people's lives based on no suspicion of criminal activity than to go after someone they suspect of a crime. While police clearly play many different roles in society, the idea that generalized surveillance would be allowed because some of those roles are not criminal in nature seems to undercut Fourth Amendment principles.[322]

*2. Reasonableness*.—A more tempting way to avoid answering whether video analytics violates the Constitution is to shift Fourth Amendment gears and focus on the "reasonableness" question.[323] The Fourth Amendment is not only concerned with threshold search questions. Reasonableness has also

320. The focus of the Real-Time Crime Center is investigating *crime*. *See, e.g.*, Michael Gallensberger, *Gary Police Department Unveils Real Time Crime Center*, LAKESHORE PUB. MEDIA (Nov. 21, 2023, 6:53 PM), https://www.lakeshorepublicmedia.org/local-news/2023-11-21/gary-police-department-unveils-real-time-crime-center [https://perma.cc/VE7F-EH9E] ("[The RTCC technology] allows all of our officers and investigators to actually get things in real time, so we can actually clear up and solve crimes at a much clearer and consistent basis."); Bria Bolden, *How 'Connect 2 Memphis' Works: A Look Inside MPD's Real Time Crime Center*, ACTION NEWS 5 (Dec. 18, 2023, 10:54 PM), https://www.actionnews5.com/2023/12/19/how-connect-2-memphis-works-look-inside-mpds-real-time-crime-center/ [https://perma.cc/VC4E-QYGC] ("People are skeptical because they think 'Big Brother' is watching, . . . That's not what we're doing. We developed this program to help our city stay safe and reduce our crime numbers.").

321. *See* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 158–61 (2017) (discussing how generalized suspicion distorts Fourth Amendment doctrine around probable cause and individualized suspicion).

322. The Supreme Court's most recent foray into the subject suggests that the Court will keep the exception narrow. *See Caniglia*, 144 S. Ct. at 1598 (concluding that the community caretaking exception does not create "a standalone doctrine that justifies warrantless searches and seizures in the home").

323. *See Brigham City*, 547 U.S. at 403 ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'"). *See generally* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977 (2004) (discussing the history of reasonableness from the Founding Era on).

been a way to respond to arbitrary or overbroad police actions.[324] The focus on reasonableness has been an ongoing battle between conservative and progressive justices, with questions about reasonableness no clearer than what a search is.[325] That said, when it comes to programmatic surveillance systems—like video analytics in all its forms—the reasonableness argument offers a way forward.[326]

A reasonableness argument would look at a system of video surveillance and ask whether such a public safety system is reasonable.[327] The analysis is akin to special needs searches[328] and the balancing test that the Supreme Court has undertaken in other circumstances.[329] For example, bag searches around stadiums or subways are viewed as public safety activities and not investigatory searches (even though there are literal searches occurring).[330] Generally, a special-needs reasonableness balancing looks at the stated government interest, the individual privacy invasion, and then whether the proposed action is effective to meet the stated governmental goal.[331] So, for example, security to get into the Super Bowl might require

---

324. *E.g.*, United States v. Ortiz, 422 U.S. 891, 895 (1975) ("[T]he central concern of the Fourth Amendment is to protect liberty and privacy from arbitrary and oppressive interference by government officials.").

325. Scott E. Sundby, *Protecting the Citizen "Whilst He Is Quiet": Suspicionless Searches, "Special Needs" and General Warrants*, 74 MISS. L.J. 501, 507–08 (2004) (explaining the historical and ongoing debate over whether the initial Fourth Amendment inquiry should be reasonableness or whether a warrant is present).

326. *See generally* CHRISTOPHER SLOBOGIN, VIRTUAL SEARCHES: REGULATING THE COVERT WORLD OF TECHNOLOGICAL POLICING (2022).

327. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 90–118 (2007); *see also* Slobogin, *supra* note 235, at 236 n.106 (cataloging cases); Kerravala, *supra* note 92 (outlining some uses for video surveillance, including "event monitoring, traffic control and enforcement, and hazmat response").

328. Marc Jonathan Blitz, *Third Party Records Protection on the Model of Heightened Scrutiny*, 66 OKLA. L. REV. 747, 773 (2014) ("'Special needs' searches are those that occur in a setting where 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'" (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995))).

329. *Id.* ("As the Court has noted, such 'even-handed blanket' searches are permissible in special needs searches conducted 'outside the criminal context' so long as they are justified by a 'balancing [of] the invasion of privacy [entailed by the search] against the government's strong need.'"); *see also* Kit Kinports, *The Origins and Legacy of the Fourth Amendment Reasonableness-Balancing Model*, 71 CASE W. RES. L. REV. 157, 165–69 (2020) (describing the history of reasonableness balancing).

330. John J. Miller, John T. Wendt & Peter C. Young, *Fourth Amendment Considerations and Application of Risk Management Principles for Pat-Down Searches at Professional Football Games*, 20 J. LEGAL ASPECTS SPORT 107, 109 (2010); Cathryn L. Claussen, *The Constitutionality of Mass Searches of Sports Spectators*, 16 J. LEGAL ASPECTS SPORT 153, 157 (2006).

331. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995) ("[W]hether a particular search meets the reasonableness standard 'is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'" (quoting Skinner v. Ry. Lab. Execs. Ass'n, 489 U.S. 602, 619 (1989))).

suspicionless searches of bags and persons, based on a balancing of the government interest in protecting attendees of the Super Bowl versus the limited privacy invasion of one's bag being searched. The idea is that searching everyone's bag is an effective deterrent to potential weapons or threats that could be concealed in a bag.[332]

While a citywide video analytics system is not analogous to the Super Bowl, in essence, the argument would be that citywide video analytics is not being used for law enforcement investigation, but for public safety goals more broadly. Under this argument, the benefit of increased public monitoring is high and the cost to individual privacy is low, so, on balance, the system should be allowed. Or so the argument would go. The problem, of course, is that the video analytics system in a Real-Time Crime Center is designed for law enforcement investigation and the privacy invasion of being tracked in public is quite substantial.[333] In addition, the efficacy argument fails to justify surveillance, because far more innocent people will be tracked than suspicious people. As a percentage of people caught in the cameras, the vast majority of people and objects will not be involved in criminal wrongdoing.

Beyond a "special needs" lens, video analytics might be unreasonable by virtue of being too generalized. Such an argument finds support in the Fourth Amendment's historical prohibition against general searches and the arbitrary and unparticularized nature of the information collected.[334] Police are using the cameras to scan everyone without a reason to believe criminal activity is occurring. The ability to surveil at a mass scale without any suspicion is the type of governmental power that gave rise to the Fourth Amendment in the first place.[335]

---

332. Miller, Wendt & Young, *supra* note 330, at 108.

333. Tyre, *supra* note 2 ("A real time crime center is a centralized location with dedicated personnel that utilize various systems and technologies to analyze disparate data sets and provide information and support to law enforcement operations. . . . [through] data gathering, analysis, and sharing information to aid in decision making and response coordination.").

334. Martin, *supra* note 53, at 727 ("[T]he Fourth Amendment does not only protect your right to keep intimate information away from police eyes; it also protects you from investigations into crimes for which police have no particularized reason to suspect you.").

335. *See* James J. Tomkovicz, California v. Acevedo*: The Walls Close In on the Warrant Requirement*, 29 AM. CRIM. L. REV. 1103, 1134 (1992) ("The Framers objected to general warrants and writs of assistance because they resulted in arbitrary deprivations of privacy, property, and liberty. Those deprivations were . . . . arbitrary and dangerous because agents of the executive were given 'unlimited discretion' to choose whom, where, and what to search and seize." (footnotes omitted)); Clancy, *supra* note 281, at 309 ("The Fourth Amendment was a creature of the eighteenth century's strong concern for the protection of real and personal property rights against arbitrary and general searches and seizures.").

In addition to being general (in that video analytics collects too much), the pattern-matching predictions are also not particularized.[336] Here, the focus is on the predictive validity of pattern matching for objects and anomalies. By design, the predicted behaviors are not individualized to a suspect.[337] The predictions and matches are instead based on other people's past acts, or past statistics, or even just a computer engineer's conjecture about what might be suspicious in the future, and coded by programmers into a system years before anything will actually alert.[338] The preprogrammed objects or anomalies may be based on hunches, biases, or theories having no scientific basis that some collection of pixels is suspicious or not.[339] And when used, by definition, the predicted anomalies have nothing to do with the individual person being alerted to.[340] Because the programming happens well before the use, every alert of suspicious behavior is generalized, unparticularized, and based on stale data. Again, this reasoning suggests that use of video analytics could be deemed unreasonable, even under a straight reasonableness analysis.

## Conclusion

Video analytics changes the way police see the world. Digitizing objects in video streams allows police new tracking and surveillance capabilities. Without question, the growth of video analytics in Real-Time Crime Centers alters expectations of privacy in public.

This Article has attempted to offer three core insights about video analytics: first, that the current Fourth Amendment doctrine does not resolve

336. One of the core limits of the Fourth Amendment is the requirement of individualized, particularized suspicion. *See* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 533 & n.206 (1995) ("Individualized suspicion of illegal activity is normally required as one element of that justification [for the interference of liberty that results from a seizure]."); *see also* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 582 (2017) ("What, then, would a warrant scheme look like in the context of tracking an individual in public? How can the particularity requirement of the Fourth Amendment be met when . . . the place to be searched . . . may be every place the target goes over the course of a month?").

337. The predictions are also likely coded with the biases of the developers. Jessica M. Eaglin, *When Critical Race Theory Enters the Law & Technology Frame*, 26 MICH. J. RACE & L., Winter 2021 Special Issue, at 151, 160 ("Understanding race and technology as both inherently social phenomena encourages a more critical eye that denounces the assumed objectivity of a tool.").

338. Shaun B. Spencer, *Predictive Surveillance and the Threat to Fourth Amendment Jurisprudence*, 14 I/S: J.L. & POL'Y INFO. SOC'Y 109, 131 (2017) ("The *Carpenter* decision could significantly impact how future courts approach predictive surveillance.").

339. Chokshi, *supra* note 122 ("Video analytics software is often trained on publicly available footage, such as YouTube videos, but there may be bias in the kinds of people who post them or in what such videos show.").

340. Jessica M. Eaglin, *Predictive Analytics' Punishment Mismatch*, 14 I/S: J.L. & POL'Y FOR INFO. SOC'Y 87, 96 (2017) (analyzing the dangers of prediction in the criminal legal system).

the question of reasonable expectations of privacy from citywide systems of mass surveillance using video analytics technology. Second, that principles emerging from the Supreme Court's "digital is different" cases suggest that such system-wide surveillance is a Fourth Amendment search. Third, because no warrant can practicably be obtained before the AI-powered pattern matching analysis runs on the system and no exception to the warrant requirement applies, use of video analytics in a Real-Time Crime Center violates the Fourth Amendment. If this analysis is correct, police may be precluded from using BriefCam or similar video analytics technologies that allow instantaneous or continuous pattern matching or object recognition. This would mean that police could not use the power of video analytics to conduct virtual patrols for objects, people, or movements.

Video analytics in Real-Time Crime Centers also changes the way we see the Fourth Amendment. First, and most obviously, the analysis in this Article shows the gaps in doctrine developed in an analog era. Applying human-centric, analog precedent to powerful digital surveillance systems makes little sense. Digital is not only different; it requires a different legal framework. Second, and relatedly, the difference in scale and scope of new AI-driven surveillance systems cannot be equated to traditional police tools. Systems of surveillance present different privacy harms, so cases that relate only to police tools are unhelpful precedent. The continuous nature of data collection, the temporal distortions of retrospective access, the preprogrammed predictive alerts, and the ability to track persons and objects through time, all upend traditional Fourth Amendment doctrine. Third, the application of the Fourth Amendment to video analytics presents a helpful test case to examine how a reimagined Fourth Amendment might protect against new privacy threats, even if questions remain.

Despite the difficulty, the necessity of applying the Fourth Amendment to new policing technologies also becomes evident. Avoiding the Fourth Amendment search question does not solve the underlying problem of too-permeating surveillance systems. While it might be tempting for courts to escape the doctrinal mess of current Fourth Amendment principles, the resulting absence of constitutional protections will have grave consequences for privacy. In the absence of legislative limits, the Fourth Amendment offers a necessary check against arbitrary or overreaching police surveillance powers. This Article offers an analytical way forward to create that check and expose the privacy harms of citywide video analytics systems.