2025

Video Analytics and Fourth Amendment Vision

Andrew Guthrie Ferguson

VIDEO ANALYTICS AND FOURTH AMENDMENT VISION

Andrew Guthrie Ferguson[*]

ABSTRACT

What does the Fourth Amendment have to say about video analytics running on city-wide camera systems?

Video analytics (also known as computer vision) involves hardware and software in cameras that turns 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 city-wide 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

[*] Professor of Law, American University Washington College of Law. 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 my student at AUWCL and Mert Karakya at IPVM.

assumptions that may need reexamination in 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]

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 turns 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

---

[1] Zac Larkman, *The Quiet Rise of Real-Time-Crime Centers*, WIRED (July 28, 2023) https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/; *see also* Electronic Frontier Foundation, *Atlas of Surveillance*, https://atlasofsurveillance.org/real-time-crime-centers (listing cities with real time crime centers).; Jahd Khlil, *Real Time Crime Centers which Started in Bigger Cities, Spread Across America*, NPR (Aug. 16, 2023) (estimating the current number of RTCCs at 135 and growing).

[2] *The Technology that Powers Real Time Crime Centers*, POLICEONE (Sept. 27, 2023) https://www.policemag.com/technology/article/15635270/how-technology-powers-real-time-crime-centers ("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*, STATE SCOOP (Aug. 24, 2023) https://statescoop.com/real-time-crime-centers-police-privacy/ ("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*, AP (Dec. 18, 2023) ("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.*, *Response Times*, STATETECH (July 19, 2022); Jim McKay, *Crooks Can't Dodge the Real-Time Crime Center 'Double Click*,' GOVT TECH (Dec. 7, 2023); Elena Barrera, *'Nerve Center': Real-Time Crime Center Helps Solves Cases in Hours Instead of Days*, TALLAHASSEE DEMOCRAT (Sept. 16, 2023).

[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 ("In a corner of the Spokane County Sheriff's Office, an array of 11 wall-mounted TV screens displayed live maps with icons tracking 911 calls and officers, social media posts and various video camera feeds – ranging from county buildings and busy intersections to a car wash and a construction site. … The sheriff's office also has another powerful new surveillance tool: $150,000 "video analytics" software that uses machine learning to scrub through days of footage in minutes and make it searchable using descriptive keywords.").

[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 4 (RAND Corp. 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 (5th Ed.), 122 BUTTERWORTH-

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, men carrying umbrellas (or other objects) and track that identified person or thing back in time across the cameras.[9] In addition, automated prompts can be programmed to identify objects (a gun, a backpack) or unusual patterns of activity (for example, 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

---

HEINEMANN (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, 15 (2021) ("The term "artificial intelligence" or "AI" refers to an aspirational goal (or the dystopian outcome) of exploring the limits of computation. The examples above of what computers can now do are generally referred to as "narrow" or "weak" AI, because they use purpose-built hardware and/or software systems that seek to emulate (or better) human performance at a single, well-defined task. "General" or "strong" AI refers to a computer's ability to rival or exceed human performance at a full complement of cognitive tasks, including but not limited to, the ability to sustain itself (*i.e.*, the task of *go forth and multiply*)."); *See, e.g., What Is Video Analytics?*, BriefCam, https://www.briefcam.com/technology/video-analytics [https://perma.cc/2WCQ-UHWH].

[7] Jay Stanley, ACLU, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, 3, 17-19 (2019) ("The goal of this technology is to allow computers not just to record but also to understand the objects and actions that a camera is capturing. This 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, Polity Press, 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, Chapman & Hall, 75 (2018) ("Object classification detects moving objects in a video sequence and classifies them into categories such as humans, vehicles, birds, clouds, or animals.").

[9] Erin Tracy, *Not Just Surveillance: Riverbank's New Cameras Recognize When You're Up To No Good*, MODESTO BEE (June 25, 2019) ("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.").

[10] Erin Tracy, *Not Just Surveillance: Riverbank's New Cameras Recognize When You're Up To No Good*, MODESTO BEE (June 25, 2019) ("Riverbank's newest surveillance cameras go beyond simply capturing video footage. They 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.").

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

---

[11] Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 717 (2017) ("[T]he tracking technology, BriefCam, allows law enforcement to overlay hours of video and then isolate individuals based on certain factors so monitors can view all applicable targets with hours of time reduced to minutes. . . . With such technologies, police could 'reverse-engineer' location tracking, picking a route they want to monitor, then use BriefCam to immediately isolate and identify everyone who used it over the course of several hours." (footnotes omitted)).

[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 be addressed. *See* Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180, 206 (2020) (discussing Brady issues with city-wide 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] Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. Rev. 1143, 1154 (2022) (describing the lack of legislative protections for new forms of surveillance technology).

[15] 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 ("Police credit new technology with helping solve crimes amid heightened public safety concerns, but on 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.").

[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. *States Push Back Against Use of Facial Recognition by Police*," USNEWS, May 5, 2021, https://www.usnews.com/news/politics/articles/2021-05-05/states-push-back-against-use-of-facial-recognition-by-police; Nicol Turner Lee & Caitlin Chin-Rothman, *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 ("[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*. https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes.

[17] "Nicol Turner Lee & Caitlin Chin-Rothman, *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-

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, scale, and general questions about expectations of privacy in public all become heightened when the Fourth Amendment is forced to confront city-wide systems of digital video surveillance.[20] In fact, as I will argue, the rise of video analytics both presents 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 city-wide Real-Time Crime Centers, although the analytics technology can be used on video streams from police body cameras, private residential surveillance cameras, private commercial 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

---

an-imperative-for-communities-of-color/#top62 ("Although facial recognition meets few enacted legal restrictions at the federal level, over seven states and 20 municipalities, such as Boston, San Francisco, and Virginia, have established some limitations on government use of facial recognition usage in certain contexts.").

[18] *See infra* Part II.

[19] Rebecca Crootof et. al., *Humans in the Loop*, 76 VAND. L. REV. 429, 440 (2023) (describing the concept).

[20] These terms will be discussed *infra* but questions about whether algorithms will make decisions without humans (humans not in the loop), 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.

[21] *See e.g.*, Jennifer A. Kingston, *New AI Tool Instantly Analyzes Police Bodycam Footage*, AXIOS (Jan. 30, 2023) ("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 Takashashi, *ZeroEyes Uses AI and Security Cameras to Detect Guns in Public and Private Spaces*, VENTURE BEAT (July 31, 2023); Douglas McMillian, *Eyes on the Poor: Cameras, Facial Recognition Watch over Public Housing*, WASH. POST (May 16, 2023); Matt Mencarini, *Michigan State Expands Surveillance, with an Eye Toward How Artificial Intelligence Can Help*, LANSING STATE JOURNAL, (May 12, 2023).

[22] Lawrence J. Fennelly, EFFECTIVE PHYSICAL SECURITY (5th Ed.), 133 Butterworth-Heinemann (2017).

[23] Avi Asher-Schapiro, *Privacy or Safety? U.S. Brings Surveillance City to the Suburbs*, THOMPSON-REUTERS, (May 11, 2023) (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) (describing the investigative power of video analytics on New Orleans camera systems) https://thelensnola.org/2018/12/20/holy-cow-the-powerful-software-behind-the-

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 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-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 city-wide 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.

This Part offers a two-step argument for why video analytics in city-wide 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 does not

---

citys-surveillance-system/.

[25] *See Paris 2024 Olympics*: *Concern over Frensch Plan for AI Surveillance*, BBC (July 18, 2023) (discussing anomaly bag detection video technologies).

[26] Jim McKay, *Crooks Can't Dodge the Real-Time Crime Center 'Double Click*,' GOVT TECH (Dec. 7, 2023) ("The center made its debut in May 2022 and combined existing resources with a new Genetec Security Center platform that leverages hundreds of cameras the department already had. 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), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-manycameras-precrime.

[27] *See infra* Part II.B (discussing cases)

[28] *See infra* Part II.C (discussing cases and scholarship)

[29] As will be discussed in Part 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, 281–82 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

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 farther, 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. Specially, 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 has consequences to Fourth Amendment theory, because the puzzle of fitting a new technology to an old law reveals gaps that need to be addressed. As more centralized city-wide surveillance systems get developed, 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 but one of the many surveillance tools embedded in these centralized surveillance systems.[34] The fact that police are centralizing the many difference surveillance capabilities into one system of social control is its own separate concern.[35] Second, this Article focuses on the Fourth

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

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

[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. Avi Asher-Schapiro, *Privacy or Safety? U.S. Brings Surveillance City to the Suburbs*, THOMPSON-REUTERS, (May 11, 2023) ("According to training materials and pitch documents obtained through public records requests, cities 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 city-wide suspicionless surveillance also violates the Fourth Amendment. Andrew Guthrie Ferguson, *Structural Sensor*

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 the dominant organizing principle of modern policing without 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 sections detail the technical specifics of how video analytics works. The third section details how police use video analytics technology in practice. Understood properly, what is happening behind the video scenes has direct impacts 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

Surveillance, 106 IOWA L. REV. 47, 53 (2020) (discussing how city-wide sensors 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 et. al., *Policing Police Tech: A Soft Law Solution*, 37 BERKELEY TECH. L.J. 705, 717 (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 (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 such legislative fixes are difficult).

[39] Eric Lander and Alondra Nelson, "ICYMI: WIRED (Opinion): *Americans Need a Bill of Rights for an AI-Powered World*," The White House Office of Science and Technology (blog), October 22, 2021, https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/.

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 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 about the types of video analytics varies widely, as does 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

---

[40] Much of the information about video analytics 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* https://ipvm.com/about. IPVM Team, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("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, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("[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] Jordy Booth et. al., DEMYSTIFYING INTELLIGENT MULTI-MODE SECURITY SYSTEMS, (Intel) APress (2023) at 66 ("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 forgoing discussion focuses on video analytics in 2024, recognizing the long history of machine learning and video. Jill Walker Rettberg, MACHINE VISION: HOW ALGORITHMS AND CHANGING THE WAY WE SEE THE WORLD, Polity Press, 5 (2023) (recognizing that machine learning was first used in image recognition in 1957).

[44] IVPM 2023 Video Analytics Book at 64 ("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. Jay Stanley, ACLU, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, 3-9 (2019). In addition, with next generation AI, video analytics will be able to do contact aware searches that will be driven and generated by the AI itself. *See* https://arxiv.org/pdf/2404.07887

[46] Adam Zewe, *Can Machine-Learning Models Overcome Biased Datasets?*, MIT NEWS, (Feb. 21, 2022) ("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.").

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 a pattern matching in real time.

B. Video Analytics: A Primer

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

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 contrasts light and dark and find the rectangular edges.[51] To find a match of the object, the algorithm will search for similar edges and similar contrasts in the dataset it was trained on to recognize objects we know as a door.[52] If we were talking about a brightly colored door, the system would break down the pixels into colors

---

[47] Jordy Booth et. al., DEMYSTIFYING INTELLIGENT MULTI-MODE SECURITY SYSTEMS, (Intel) APress (2023) 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.").

[48] IPVM Team, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals.

[49] *Id*.

[50] *Id*.

[51] *Id*.

[52] Jordy Booth et. al., DEMYSTIFYING INTELLIGENT MULTI-MODE SECURITY SYSTEMS, (Intel) APress (2023) 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. Classification is measured in inferences/second. Identifying one object equals one inference.").

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 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 all the need to label millions of objects for training sets.[60] Relatedly, perhaps if the only information you need is whether the door is opened or closed a

[53] IVPM 2023 Video Analytics Book at 100 ("When color analytics are being used as a second step analyze metadata from the camera's imager, to view numeric representations of pixel color."); *see generally* Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 695–96 (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. One pixel, then, might be coded as (240, 0, 120); that is, it takes a red value of 240, a green value of 0, and a blue value of 120.").

[54] Maheshkumar H. Kolekar, INTELLIGENT VIDEO SURVEILLANCE SYSTEMS: AN ALGORITHMIC APPROACH, CHAPMAN & HALL, 75 (2018) ("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) https://www.wired.com/story/millions-of-workers-are-training-ai-models-for-pennies/.

[56] IVPM 2023 Video Analytics Book 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."); Jordy Booth et. al., DEMYSTIFYING INTELLIGENT MULTI-MODE SECURITY SYSTEMS, (Intel) APress (2023) at 66 ("The 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. This method works well when the object is well defined and the scene is well understood or controlled. However, as the number of objects increases or the scene conditions vary widely, it becomes increasingly difficult for the developer to predict the critical features that must be detected to identify an object.").

[57] IPVM Team, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("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, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("In unsupervised learning, the images are not labeled, and the computer decides how to group the objects.").

[59] Josh Dzeiza, *AI is a Lot of Work*, THE VERGE (June 20, 2023) (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. 3, 2023).

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 objects.

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.[63] And even with the most sophisticated of deep learning data sets, the training process happens before the video camera is deployed in the field.[64] 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.[65] 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. Finding a dataset of accurately identified guns is critical to accurate pattern

---

[61] IPVM Team, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("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)"); Maheshkumar H. Kolekar, INTELLIGENT VIDEO SURVEILLANCE SYSTEMS: AN ALGORITHMIC APPROACH, CHAPMAN & HALL, 75-76 (2018) (describing the differences between shape-based classification and movement-based classification).

[62] Mert Karakaya, *The Future of Video Analytics – CNNs vs. VIT (Visual Inference Transformers*), IPVM Reports (Jan. 5. 2024).

[63] 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 ("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. ("HOG stands for "histogram of oriented gradients" and detects objects by finding edges and corners in an image, and how strong/sharp the edges and corners are. Feature descriptors are applied to the simplified image and can be programmed to detect the car, persons, or specific details like the license plate, by using the features to find edges. Because of this, HOG can be more accurate than Haar at some tasks, and less prone to errors due to lighting and angles compared to Haar.").

[64] IPVM Team, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("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.").

[65] IPVM Team, Video Analytics Fundamentals Guide, (Mar 04, 2021 11:00 AM) https://ipvm.com/reports/analytics-fundamentals ("Datasets are used to train deep learning analytics on how to detect or recognize persons, vehicles, behaviors, faces, or any object/action. Datasets are typically composed of thousands to millions of labeled images or videos.").

matches. Common datasets exist that allow for object recognition training.[66] Well known datasets like COCO, ImageNet or Pascal2 offer centralized training sets of all sorts of common images available to purchase.[67] 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.[68] 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 of Black and Brown women (or really anyone who did not fit the training data).[69] Similarly, 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.[70]

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, 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 predicable 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, with different lighting

---

[66] Kent Gauen, Ryan Dailey, John Laiman, Yuxiang Zi, Nirmal Asokan, Yung-Hsiang Lu, George K. Thiruvathukal, Mei-Ling Shyu, and Shu-Ching Chen, *Comparison of Visual Datasets for Machine Learning*, Proceedings of IEEE Conference on Information Reuse and Integration 2017 (describing various datasets).

[67] *Id*.

[68] Maheshkumar H. Kolekar, INTELLIGENT VIDEO SURVEILLANCE SYSTEMS: AN ALGORITHMIC APPROACH, CHAPMAN & HALL, 81-86 (2018) (for a technical description of how convolutional neural networks (CNN) work for object recognition).

[69] 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);; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 11 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/Z2XX-GSB3].

[70] Dave Maass & Matthew Guariglia, *Video Analytics User Manuals Are a Guide to Dystopia*, EFF (Nov. 19, 2020) ("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.").

conditions and angles.[71] A moving bicycle might look different than a static image, making pattern recognition more difficult.[72] Training algorithms on 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 city scape, 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 everything 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.[73] More traditional optical character recognition (OCR) algorithms take characters as inputs and matches the edges to identify the letters or numbers.[74] For example, the edges that create the recognizable numbers 1234 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.[75] 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.).[76] Once digitized, the different points can be matched to

---

[71] IVPM 2023 Video Analytics Book at 138 ("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.").

[72] *See also* NIST testing on the problem. file:///C:/Users/aferg/Downloads/Phase3_ActEV_2021_SDL_EvaluationPlan_20210803.pdf/

[73] *See* Jill Walker Rettberg, MACHINE VISION: HOW ALGORITHMS ARE CHANGING THE WAY WE SEE THE WORLD, Polity Press, 83-115 (2023) (discussing the use of ALPRs): Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 610 (2024) (discussing the rise of automation in ALPR technology).

[74] IVPM 2023 Video Analytics Book at 139 ("OCR (Optical Character Recognition) takes a single character as an input, and either matches it against complete characters or turns the character into pieces and matches those pieces against patterns for characters. 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'.").

[75] IVPM 2023 Video Analytics Book at 138 ("While LPR 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.").

[76] Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, Georgetown L. Ctr. on Priv. & Tech., *The Perpetual Line-Up: Unregulated Police Face Recognition in America* 1 (2016) [https://perma.cc/S48P-PL53]. Michael Kwet, *The Rise of Smart Camera Networks, and Why We*

identify similar features and thus identify people.[77] "Traditionally, facial recognition technology has been "feature-based," which utilizes identifying measures like one's eyes, nose, and mouth and the distances between these 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."[78] Once faces are turned into a digital faceprint (like a digital fingerprint), they can be matched to a database of stored digital faceprints.[79] Algorithms match the commonality of the probe photo to the database of photos and as an output produce a selection of close matches. With video surveillance, facial recognition is more complicated (and less reliable) because issues lighting, angle, and limited video quality can interfere with matching.[80] Several false arrests have occurred using facial recognition.[81] The result has been that video analytics companies have relied on more powerful neural networks to try to improve on accuracy for facial recognition.[82]

Other use cases for video analytics involve bag detection (backpacks, suitcases), unusual movement detection, and anomaly detection.[83] In these

---

Should Ban Them, THE INTERCEPT, (Jan. 27. 2020) ("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.").

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

[78] 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 (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).

[79] *See also* Joy Buolamwini, Vicente Ordóñez, Jamie Morgenstern & Erik Learned-Miller, *Facial Recognition Technologies: A Primer* 8-13 (2020), https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66al4_FRTsPrimerMay2020.pdf [https://perma.cc/X8CH-JAV3].

[80] IVPM 2023 Video Analytics Book Aa 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.").

[81] 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].

[82] IVPM 2023 Video Analytics Book at 130 ("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.")

[83] Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM.

situations, the object recognition is trained to recognize an out of place suspicious bag (suggesting the possibility of a bomb), or movement in crowds that are unusual (perhaps someone entering via an exit), or some unusual movement (perhaps a bright light in a location that would ordinarily be dark).[84] The programing of such alerts involves programing an alert system to recognize a pattern that does not fit the expected scene.

Finally, video analytics can be used for behavior identification, such as when particular movements are identified to correspond to particular pre-programmed patterns of activity.[85] For example, video analytics has been trained to recognize an altercation or a robbery based on training of videos of fights or convenance store robberies.[86] While more prone to error because of the complexity of matching behaviors (the difference between a physical assault and a loving bear hug greeting is understood in context), the use for public safety management is evident.

The above list is not exclusive, 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.[87] The next section 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 Command Center populated by active-duty

---

& 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.").

[84] *See e.g.*, Mohammad Ibrahim Sarker et. al., *Semi-Supervised Anomaly Detection in Video Surveillance Scenes in the Wild*, SENSORS (Basel) (June 21, 2021) ("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.") https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8230050/

[85] IVPM 2023 Video Analytics Book at 110 ("The most common method for building behavior recognition systems is human defined rules based on pose estimation, object detection, and other data to trigger alerts. Developers define what activities of interest are, as in the example above (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.").

[86] Some companies advertise the ability for their video analytics to identify violence. *See e.g.*, https://oddity.ai/

[87] IVPM 2023 Video Analytics Book 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* IVPM 2023 Video Analytics Book 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,[88] Chicago, Illinois,[89] or Savannah, Georgia[90] police officers sit watching video screens. The screens have video analytics like BriefCam[91] (or the equivalent) technology running behind the scenes able to sort, search, and identify objects.[92] Some cities like Chicago have over 32,000 linked cameras offering police access to many parts of the city.[93] Some companies, like Fusus, envision linking tens of thousands of public and private cameras together in a single Real-Time Crime Center.[94] Other cities have less expansive coverage, choosing to focus on downtown areas, "high crime areas," or other places with cameras installed.[95] The technology now exists to link private security cameras and city security cameras and law enforcement cameras, providing police a live feed through

[88] Eoin Higgins, *Pre-Crime Policing Is Closer Than You Think, and It's Freaking People Out*, VICE (June 12, 2018), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-manycameras-precrime; Zeus Kerravala, *Fact of Fallacy: Video Cameras Are More than Just Another Set of Eyes*, STATE TECH MAGAZINE (July 24, 2023) ("[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.") https://statetechmagazine.com/article/2022/07/fact-or-fallacy-video-cameras-are-more-just-another-set-eyes.

[89] 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.

[90] Jake Shore, *What to Know: New Savannah Police Technology Can ID Suspects by Clothes, License Plates*, GEORGIA PUBLIC BROADCASTING (Oct. 27. 2022) ("[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.") https://www.gpb.org/news/2022/10/27/what-know-new-savannah-police-technology-can-id-suspects-by-clothes-license-plates.

[91] BriefCam, https://www.briefcam.com/technology/video-analytics/; Caroline Haskins, *Many Police Departments Have Software that Can Identify People in Crowds*, BUZZFEED (June 12, 2020) ("Authorities in Chicago; Boston; Detroit; Denver; Doral, Florida; Hartford, Connecticut; and Santa Fe County, New Mexico have also used [BriefCam].")

[92] BriefCam, *How it Works*, https://www.briefcam.com/technology/deep-learning/.

[93] Tammy Webber, *Chicago's Vast Camera Network Helped Smollett Investigation*, AP (Feb. 22, 2019) (describing 32,000 cameras); Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018).

[94] Joseph Cox, *Is Your Local Police Department Using FUSUS AI Enabled Cameras?*, 404 MEDIA (Jan. 16. 2024) ("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.") https://www.404media.co/fusus-ai-cameras-map-local-police/. In 2024, Fusus was bought by Axon, a large platform provider of body cameras and digital storage.

[95] *Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, WALL ST. J. VIDEO (May 30, 2019, 5:30 AM), https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517AE31BE3C5E7E.html [https://perma.cc/HX8A-ZJ5J]. *See* Zac Larkman, *The Quiet Rise of Real-Time-Crime Centers*, WIRED (July 28, 2023) https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/ (discussing the rise of RTCC cameras).

this growing network.[96] The reality of video analytics is that it can simply be run on top of this network of 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 technology 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 digital 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.[97] 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.[98] 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.[99] Live monitoring need not require any use of video analytics running behind the scenes (although it might). Police – as human observers – can just watch the camera feeds and then send in human police officers to investigate.

This human monitoring is different and distinct from automated

---

[96] The numbers of cameras are high and growing. For example, Atlanta has over 24,000 cameras, Philadelphia, Pennsylvania has 28,000, San Fransisco has 14,000, even Denver, Colorado has 12,000. *See* Jurgita Lapienyte, *This is the Most Heavily Surveilled City in the US: 50 CCTV cameras per 1000 Citizens*, CyberNews, (Nov. 15, 2023) https://cybernews.com/editorial/this-is-the-most-heavily-surveilled-city-in-the-us-50-cctv-cameras-per-1000-citizens/.

[97] Avi Asher-Schapiro, *Privacy or Safety? U.S. Brings Surveillance City to the Suburbs*, THOMPSON-REUTERS, (May 11, 2023) ("Rialto is betting big on cameras: from 2020 all newly constructed or remodeled commercial and industrial properties in the city were required by the police to register cameras in the Fusus system and allow police to access a live-view, according to the police department. Police in Rialto want to be able to draw a circle on a map of the city, and automatically pull up security camera feeds from cameras in that 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.").

[98] *Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, WALL ST. J. VIDEO (May 30, 2019, 5:30 AM), https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517AE31BE3C5E7E.html [https://perma.cc/HX8A-ZJ5J].

[99] Michael Isaac Stein, '*Holy Cow': The Powerful Software Behind the City's Surveillance System*, THE LENS (Dec. 20, 2018) (describing the investigative power of video analytics on New Orleans camera systems) https://thelensnola.org/2018/12/20/holy-cow-the-powerful-software-behind-the-citys-surveillance-system/; Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT, (Jan. 27. 2020) ("Object recognition can recognize faces, animals, cars, weapons, fires, and other things, as well as human characteristics like gender, age, and hair color.").

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.[100] 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.

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 command center, software does the watching confident that the objects and movements being captured are recorded and searchable. Law enforcement has embraced this surveillance both for its scale to expand search capabilities, but also because it reduces human police presence on the streets. 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 seek 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.[101]

Again, two forms of video investigation are possible. In the first, a human police officer can just roll back the video to find the video of an incident. If police report 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.[102] This is 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.

In the second situation, police can investigate the incident using the analytical power of the stored digital images.[103] Essentially, the entire city

---

[100] BriefCam Blog, https://www.briefcam.com/resources/blog/object-detection-and-identification-in-video-analytics/

[101] Heather Kelly & Rachel Lerman, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, Wash. Post (June 3, 2020, 4:00 AM), https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/ [https://perma.cc/53ZG-9YKA].

[102] *Video Analytics Solutions for Post-Event Investigations*, BriefCam, https://www.brief-cam.com/solutions/police-investigations/ (last visited March 2, 2021) [https://perma.cc/JZ2L-KZPW].

[103] Milestone Systems, *Hartford Crime Center Expands Surveillance*, YouTube (Dec. 12, 2017), https://www.youtube.com/watch?v=OlGxTITe6dE [https://perma.cc/7F8W-T6DW].

under video surveillance has been captured in digital code, and police have the capacity to find a particular object within the data.[104] If that object is a person who committed a robbery, police have the ability to both search via data 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.[105]

A rather sensational example happened in Chicago, when the actor Jusse 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.[106] 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.[107] 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.[108] As was described by the chief of the Chicago Police Departments technology section, "Video 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."[109] It was then that the story fell apart and it turned out that Smollett had paid the two men money to stage the assault. Evidence detailing their involvement in the hoax led to criminal charges against Smollett.[110] This type of *ex post* investigation can happen

---

[104] Avi Asher-Schapiro, *Privacy or Safety? U.S. Brings Surveillance City to the Suburbs*, THOMPSON-REUTERS, (May 11, 2023) ("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 id*. ("The number of public and private surveillance cameras in use grew from 70 million in 2018 to 85 million in 2021, industry research group IHS Markit has found.")

[105] Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT, (Jan. 27. 2020) ("Using a feature called Video Synopsis, BriefCam overlays footage of events happening at different times as if they are appearing simultaneously. For example, if 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.").

[106] 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.

[107] *People v. Smollett*, 2023 IL App (1st) 220322, ¶ 10.

[108] *See* BriefCam, Resources, https://cdn2.hubspot.net/hubfs/3916087/Resources/BriefCam%20At%20Work%20in%20Safe%20Cities.pdf.

[109] *Id*.

[110] Tammy Webber, *Chicago's Vast Camera Network Helped Smollett Investigation*, AP (Feb. 22, 2019) ("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

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.[111] 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 (a blue car) in the city. The images can be superimposed on the screen so multiple objects can be viewed simultaneously. Because location allows inference about identity (home, work, friend 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.[112]

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.[113] 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 something that does not fit the pre-programmed pattern and an alert is signaled.[114]

Anomaly detection is not yet used in many policing systems because making predictions about city-wide patterns can be difficult.[115] To work

approach to public safety.").

[111] Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 951 (2016).

[112] In a fascinating article, the NY 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 et al., *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/locationdata-privacy-apps.html;

[113] Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT, (Jan. 27. 2020) ("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.").

[114] Nirja Chokshi, *How Surveillance Cameras Could be Weaponized with AI*, NY TIMES (June 18, 2019) ("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 Jay Stanley, ACLU *supra note* xx).

[115] *But see e.g.*, Mert Karakaya, *How ViTs/ChatGPT Can Automatically Alert On Protests Tested*,

well, city environments would need to be predictable enough to predetermine what a suspicious event might look like ahead of time.[116] 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 – 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 movement. 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.[117]

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,[118] but setting up automated alerts for trucks along the banks of the river might be easy enough.[119] 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).

In addition, anomaly detection is valuable as a public safety measure exposing abandoned bags and other suspicious packages.[120] 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 can be used in the city environment.[121]

Finally, in the not-to-distant-future we will see "crimes" alerted to as

---

IVPM, (April 29, 2024) https://ipvm.com/reports/vits-protests (showing how police are beginning to test the technology).

[116] Dave Maass & Matthew Guariglia, *Video Analytics User Manuals Are a Guide to Dystopia*, EFF (Nov. 19, 2020) ("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."); Keely Quinlan, *Police Real-Time Crime Centers are Becoming Data Powerhouses*, STATE SCOOP (Aug. 24, 2023) https://statescoop.com/real-time-crime-centers-police-privacy/ ("While traditional police work is reactive, law enforcement's access to a continual feed of video and data makes proactive policing a growing possibility.")

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

[118] 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).

[119] Erin Tracy, *Not Just Surveillance: Riverbank's New Cameras Recognize When You're Up To No Good*, MODESTO BEE (June 25, 2019) (discussing the use of anomaly detection to identify people who dump trash along a roadway).

[120] 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.

[121] *See supra* notes xx, xx.

anomalies using AI-large language models. 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.[122] Once developed as a capability, this will give RTCC systems the ability to identify crimes from visual clues across a city. 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.[123] Further, error concerns emerge as video analytics might confuse a tackle football game as a fight or a stickball bat as a weapon.[124]

All the above use cases, however, must be qualified by the recognition that police will use the technologies in different ways against different communities.[125] Race and racialized policing have been a part of policing technology since its creation.[126] The use of new video analytics surveillance cannot avoid those same cautions. 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

---

[122] 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 ("[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.").

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

[124] *See* Mert Karakaya, *How ViTs/ChatGPT Can Automatically Alert On Protests Tested*, IVPM, (April 29, 2024) https://ipvm.com/reports/vits-protests (demonstrating how early tests of vision transformer that can identify events from video can distinguish between a fight and a dance party).

[125] *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, 15 (2023); *see generally* Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (NYU Press 2017)

[126] *See generally* Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO STATE L.J. 1103 (2020); Ngozi Okidegbe, *When They Hear Us: Race, Algorithms and the Practice of Criminal Law*, 29 KAN. J.L. & PUB. POL'Y 329 (2020); Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 441-43 (2017); Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 166.; *but see* I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1280 (2017).

the reasonable expectation of privacy analysis.[127]

A. The Search Question

The Fourth Amendment prohibits "unreasonable searches and seizures."[128] The result of this textual command has been a focus on the threshold question of whether a government agent has searched or seized something and the reasonableness with which the search or seizure was conducted.[129] A "search" is a term of art in Fourth Amendment doctrine defined either a violation of a "reasonable expectation of privacy"[130] or a physical intrusion into a constitutionally protected space with the intent to gather information.[131] If a search occurs without a warrant or an exception to the warrant requirement, a Fourth Amendment violation has occurred.[132] If 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 *ex ante* whether there was an expectation of privacy in a place, activity, or thing.[133] 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.[134] Yet, it is the existing law and must be addressed by

---

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

[128] U.S. CONST. AMEND. IV.

[129] 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 the Supreme Court has gone away from textualism with the reasonable expectation of privacy test).

[130] Katz v. United States, 389 U.S. 347, 361 (1967) (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.'").

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

[132] Arizona v. Gant, 556 U.S. 332, 338 (2009) ("Consistent with our precedent, our analysis begins, as it should in every case addressing the reasonableness of a warrantless search, 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.").

[133] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. 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.").

[134] 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,

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.[135] 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*[136] – a case involving long-term digital pole cameras – by framing the 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.
>
> 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

Katz will continue to distort Fourth Amendment jurisprudence.").

[135] This expectation also may be impacted by racial bias or social economic status. See Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1140 (2020) ("Fourth Amendment protections are limited to spaces where there is a reasonable expectation of privacy. Thus, generally, the more public the location, the less there is of an expectation of privacy. This distinction rests in part on a privileged concept of privacy, one much divorced from the realities of freedom and safety which also impact privacy. Public locations are just as much deleterious spaces as are private spaces with racialized surveillance practices.").

[136] United States v. Tuggle, 4 F.4th 505, 509 (7th Cir. 2021), *cert. denied*, 212 L. Ed. 2d 7, 142 S. Ct. 1107 (2022).

> 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.[137]

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),[138] 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 is a search, one must understand the background Fourth Amendment doctrine. In a series of cases from the 1960s-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.[139]

The canon is centered by *Katz v. United States*, the case that gave us the "reasonable expectation of privacy" test.[140] To investigate whether Charlie Katz was engaged in illegal betting, the FBI attached a tape recorder to the roof of a coin-operated, glass-enclosed phonebooth.[141] Katz's

---

[137] *Id*. at 509.

[138] *Id*. at 529.

[139] 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 "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.").

[140] *See supra* note xx.

[141] 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

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 phonebooth.[142] The Court held that a person could claim a reasonable expectation of privacy in their conversation in 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 phonebooth.[143] 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."[144] 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*, police used a fixed wing plane to fly over Ciraolo's property and observed illegal marijuana plants.[145] 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 1000 foot] altitude to obtain a warrant in order to observe what is visible to the naked eye."[146] *Ciraolo* was followed by *Riley v. Florida* which involved police using a helicopter flying at 400 feet to observe illegal marijuana growing in Riley's backyard.[147] In *Riley,* a plurality held that Riley

booth. One of the three booths was placed out of order by the FBI with the consent of the telephone company." (citations omitted)).

[142] Katz v. United States, 389 U.S. 347, 352 (1967) ("[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.").

[143] *Katz*, 389 U.S. at 361 (Harlan, J. concurring) ("The critical fact in this case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted. … The point is not that the booth is 'accessible to the public' at other times, … but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable.'').

[144] Katz, 389 U.S. at 351.

[145] California v. Ciraolo, 476 U.S. 207, 209 (1986) ("Officer Shutz, who was assigned to investigate, secured a private plane and flew over respondent's house at an altitude of 1,000 feet, within navigable airspace; he was accompanied by Officer Rodriguez. 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 a 15- by 25-foot plot in respondent's yard.").

[146] *Ciraolo*, 476 U.S. at 215.

[147] Florida v. Riley, 488 U.S. 445, 448 (1989) ("When an investigating officer discovered that he

failed to demonstrate that his expectation of privacy in his backyard was reasonable where it was not demonstrated that helicopter flights were rare in the area.[148] 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* which involved the use of a radio beeper to track a car in public.[149] The question in *Knotts* was whether someone could claim a violation of an expectation of privacy after being tracked by an electronic beeper. In upholding the use of a beeper to track suspected drug manufacturing materials, the Supreme Court stated, "A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[150] 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.[151]

Together, these statements have been read to find that individuals in public have little expectation of privacy from police observation – including video

---

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.").

[148] *Riley* involved a plurality opinion with the controlling concurrence written by Justice Sandra Day O'Connor which focused on the defendant's failure to prove that helicopters were unusual in the area. *Fla. v. Riley*, 488 U.S. 445, 454 (1989) (O'Connor, J. concurring) ("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.'").

[149] United States v. Knotts, 460 U.S. 276, 277 (1983) ("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].").

[150] United States v. Knotts, 460 U.S. 276, 281–82 (1983)

[151] *Id*.

surveillance.[152]

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.[153] 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 privacy 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 demonstrated a lack of any expectation of privacy in that information *vis a vis* the government.[154] Similarly, the Supreme Court has held that disclosures to third party individuals who later convey that information to the police undermine a reasonable expectation of privacy.[155] Such "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.[156]

The traditional Fourth Amendment canon is still controlling law and used by courts to decide issues of 21st Century surveillance.[157] 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 with public surveillance.[158] Based on this interpretation, police chiefs

---

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

[153] *See generally* 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); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574–76 (2009).

[154] Smith v. Maryland, 442 U.S. 735, 737 (1979) (third party land line phone records); United States v. Miller, 425 U.S. 435, 437 (1976) (third party bank records).

[155] *State v. Skok*, 122 A.3d 608, 615 (Conn. 2015) ("[T]he [Supreme Court] held that it was not unconstitutional under the fourth amendment for a "false friend… i.e., an individual working as an undercover agent for law enforcement, to enter the defendant's place of business and, while wired for sound, engage the defendant in a conversation wherein he made incriminating statements.").

[156] *See generally* 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, 275 (2006) (discussing false friend cases); Wayne A. Logan, *Crowdsourcing Crime Control*, 99 TEX. L. REV. 137, 154 (2020) (discussing the private search doctrine).

[157] The *Tuggle* case discussed earlier is a good example. *See supra* note xx. 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, 511 (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.").

[158] As just one stark example, in a case involving the Baltimore Police Department's use of the Persistent Surveillance System planes which could videotape the entire city at a time and record all

have publicly stated that most surveillance is allowed in public without constitutional restraint.[159] In addition, this justification has been used to surveil poor communities of color deemed "high crime" more than other communities.[160]

Read carefully, however, the Supreme Court's doctrine on privacy in public is more nuanced, justifying the analog surveillance technologies of the 20th Century, but not necessarily validating mass surveillance systems that have arisen in the 21st Century like nationwide cell site location systems, global GPS systems, or city-wide Real Time Crime Centers. It is 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.[161]

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.[162] The cases do not offer a new test, purporting to be interpreting the expectation of privacy test, but do suggest a more protective approach privacy. Two of the cases *Jones v. United States*[163] and *Carpenter v. United States*[164] directly

---

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 (D. Md.), *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, 48 (2022) (critiquing this myopic analysis).

[159] *See e.g.*, Paul Edward Parker, *Who's Watching You? New Surveillance Cameras Make Inroads in RI, Raising Privacy Concerns*, PROVIDENCE JOURNAL (Feb. 12, 2022) (discussing Flock cameras, Col. Michael J. Winquist, the police chief in Cranston "When you're on a public roadway," he said, "there's no expectation of privacy.").

[160] *See* Chaz Arnett, *Black Lives Monitored*, 69 UCLA L. REV. 1384, 1406 (2023); Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1140 (2020); Monica C. Bell, *Anti-Segregation Policing*, 95 N.Y.U. L. REV. 650, 710 (2020).

[161] *State v. Briggs*, 283 A.3d 165, 169–563 (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.").

[162] 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 not just how the information is collected and processed (digitization), but what can be done with it (datafication). *See* Ira S. Rubinstein & Bilyana Petkova, *Governing Privacy in the Datafied City*, 47 FORDHAM URB. L.J. 755, 759 (2020) ("[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.").

[163] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)

[164] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)

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 28 days was a search for Fourth Amendment purposes.[165] 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.[166] This holding did not address whether Antoine Jones had a reasonable expectation of privacy from not being tracked for 28 days. Five concurring Justices did, however, address whether Jones' public movements could be tracked via GPS for 28 days.[167] In two concurring opinions, the Justices recognized that long-term tracking – even in public – violated a reasonable expectation of privacy.[168] While it is true that police could have tracked 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*.[169] *Carpenter* asked whether an individual had a reasonable expectation of privacy from being tracked for 7 days by cell site location information (CSLI). CSLI is the location data phone companies use to track cell phones and connect them with nearby cell phone towers.[170] CSLI generates an approximate triangulated location of the cell phone user at all times.[171] 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.[172] The CSLI placed Carpenter at the robbery locations at the time of the crimes.[173] Carpenter argued that this

[165] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)

[166] *Jones*, 565 U.S. at 404–05 ("It is important to be clear about what occurred in this case: 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.").

[167] *See 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 judgment).

[168] *See id*. at 430 (Alito, J., concurring in judgment); *id.* at 415 (Sotomayor, J., concurring)

[169] 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*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.").

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

[171] *Id*.

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

[173] *See id*. at 2212–13.

collection of location data without a warrant violated his reasonable expectation of privacy and thus the Fourth Amendment.

The Supreme Court agreed with Carpenter, holding that long term location tracking violated a reasonable expectation of privacy and required a warrant.[174] This was true even though Carpenter's movements were in public.[175] This was true even though the data had been provided to a third party (the cellphone company).[176] This was true even though nothing more than his location at the robbed stores was to be introduced at trial. 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.[177]

These two "digital Katz" cases[178] 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 open many unanswered questions.

The final piece of the "digital is different" line of cases is *Riley v. California*.[179] *Riley* involved the warrantless search of a smartphone incident to arrest. In reaching its conclusion, the Court explored the difference between analog searches and digital searches. David Riley was arrested for a traffic offense and his car impounded.[180] During a routine inventory search of the car, two guns were recovered. Without a warrant, detectives investigating Riley and his possible connection with a local gang searched through his smartphone for evidence connecting him to the guns.[181] In the photo app in Riley's smartphone, police found a photograph that prosecutors used to link him to an earlier shooting. Riley filed a motion to suppress the data from his smartphone arguing that police needed a warrant to search the phone.

---

[174] *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.").

[175] All of the locations revealed were outside of Carpenter's home or private property.

[176] The records at issue were held by private cellphone companies that provided cellphone services to paying customers.

[177] Carpenter 128 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).

[178] Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (Jun. 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/

[179] Riley v. California, 573 U.S. 373, 386 (2014).

[180] *Riley*, 573 U.S. at 379.

[181] *Id*.

The Supreme Court agreed with Riley, holding that a warrant was required to search a digital device even incident to arrest.[182] 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.[183] The Court considered the privacy harms of a smartphone different than a wallet or cigarette pack recovered incident to arrest.[184] The Court specifically described why exposing data in a smartphone was qualitatively and quantitatively different from any analog cases.[185] Data in a smartphone included contacts, calendars, notes, email, texts, financial information, photos, news, other Apps, and Internet searches (among other things).[186] In statements that both acknowledged 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.[187] In Riley's case that meant that police needed a warrant

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

---

[182] *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.").

[183] *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 cellphones.").

[184] *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—nor would they have any reason to attempt to do so."); *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.").

[185] *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.").

[186] *Id.* at 393–94 ("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 a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[187] *Id.* at 396–97 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

First, 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.[188] 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).[189] The logic makes some sense. By being in public, one can expect human police officers to observe you. Especially in an era before digital surveillance systems, the only expectations one might reasonably expect at the time came from human beings. In 1967, if one was going 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). *Carpenter* and *Jones* hint at this recognition that automation and non-human capacities change the balance of police power and require greater protections.[190] As Justice Alito acknowledged in *Jones*, human officers could not have tracked

---

[188] Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 Ohio St. L.J. 817, 853 (2022) ("One of the most striking realizations in studying the early Fourth Amendment cases is how dependent the surveillance was on human agents (and agency). Whether it is the *Katz* officers physically taping the microphones on the telephone booth and turning on the device, or the *Karo* agents tracking the beeper, or police officers peering out of planes to see marijuana growing, the human was not only in the loop, but was key to the search. While the cases were nominally focused on technology and the Fourth Amendment, the reasonable expectations of privacy was still a reaction to human observation.").

[189] *Cf. Ciraolo*, 476 U.S. at 213 ("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) ("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."); *see also 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 Knotts.* 460 U.S. at 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.").

[190] *Carpenter* in fact speaks explicitly about the danger of a mechanical application of analog precedent. *See Carpenter*, 138 S. Ct. at 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." 'These efforts reflect a bipartisan consensus that, when it comes to government surveillance of private citizens, 'digital is different.'" (footnotes omitted)); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 615–16 (2011) (describing automation and what happens without human actions).

the suspect as effortlessly as GPS could because they did not have the real-world capabilities to do so.[191]

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.[192] All of the cases in the traditional canon involved surveillance tools – one-off information collection devices. Whether we are thinking of a beeper, tape recorder, thermal imager, pen register, or film camera, all the early cases involved a single-use technology that because of the technological limitations were necessarily limited in scope and scale.[193] Systems that involve many data sources and aggregating capabilities offer a different privacy harm.[194] 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.[195] The identified harm with CSLI was a nationwide system that could track anyone for any reason without a warrant and aggregate that data together.

Third, expectations of privacy have been temporal in nature, having a natural limit on the amount of surveillance possible and little ability to go back in time to uncover past clues.[196] 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 hovering helicopter etc.), but it was hard, if not impossible, to use the

---

[191] Jones, 565 U.S. at 430 (Alito, J., concurring) ("[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. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

[192] In prior work, I have analyzed how this distinction can make a difference in case outcomes. Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 38–39 (2022) ("Early Fourth Amendment cases involved tools. The thermal imaging device in *Kyllo* was a handheld device to be used by an individual agent. It was a standalone tool to measure heat levels from a particular house. Similarly, the flyover cases in *California v. Ciraolo* and *Florida v. Riley* involved ordinary cameras taking photos of individual yards. Even the "wiretap" in *Katz* was a physical recording device affixed by hand to a single phone booth. In contrast, the CSLI system in *Carpenter* was a vast network of cell towers that provided a nationwide system of data capture, and the *Jones* case involved a global satellite tracking system.").

[193] *See id*.

[194] *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).

[195] Carpenter 138 S.Ct. 396–97.

[196] In a prior article, I called this the anti-permanence principle. Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1135–36 (2021) ("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.").

accumulated data retrospectively.[197] 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.[198] In addition, viewing the tape of a CCTV camera took a long time because one had to watch the film in almost real time.[199] It was not easily searchable for objects or people. *Carpenter* and *Jones* both recognized the retrospective nature of digital surveillance and attendant harms changed the analysis.[200]

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.[201] It was easy to see when the contested "search" occurred. Traditionally, there was an affirmative action of a police officer that triggered the inquiry. 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 ongoing and continuous.[202] One of the hardest, and still likely unanswered

---

[197] *Carpenter*, 138 S. Ct. at 2218 ("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.").

[198] Carpenter, 138 S. Ct. 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.").

[199] Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT, (Jan. 27. 2020) ("In their first decades of existence, CCTV cameras were low-resolution analog devices that recorded onto tapes. Businesses or city authorities deployed them to film a small area of interest. 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."); Jordy Booth et. al., DEMYSTIFYING INTELLIGENT MULTI-MODE SECURITY SYSTEMS, (Intel) APress (2023) at 8 ("Before the 2000s, typical [camera security systems] were built around analog cameras; the recordings they made were spooled to VHS tapes on stand-alone systems. When an incident occurred, a security agent faced a time-intensive process of screening VHS tapes on a video monitor to find an incident. Sharing the 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.").

[200] *Id*.; *see also* 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))

[201] *See* Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 17 (2022) ("Continuous automation creates a more complicated reality for analysis. For example, in a traditional Fourth Amendment case, the act analysis was rather straightforward to apply. First, there was almost always a government agent acting in a specific, singular manner…· 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.").

[202] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 615–16 (2011).; Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 596 (2024).

questions in *Carpenter* was when did the search occur.[203] 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).[204] Is there no search until the government acquires the information, even though the data collection relevant to the case happens earlier? 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 technology – 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 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.[205]

The Article argues that video analytics running on these city-wide surveillance systems violates a reasonable expectation of privacy and is a search for Fourth Amendment purposes. Properly understood, the technology powering video analytics – be in virtual patrols, retrospective investigation, or anomaly detection – involves continuous, wide-scale, suspicion-less object recognition matching without a warrant. Put simply, to work as designed, video analytics must be searching everything everywhere all at once to pattern match and categorize the objects (including persons and effects) in its computer vision.[206]

---

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

[204] 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.").

[205] Many scholars have also attempted to craft Fourth Amendment arguments about a privacy in public. *See 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, 6 (2007); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 682 (2013)

[206] Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT, (Jan. 27. 2020) ("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.

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.[207] This first step posits that – at a minimum – courts cannot rely on the traditional analog canon to resolve the Fourth Amendment search question. Nothing in the existing doctrine answers the constitutional question, and it is an error to equate video analytics with traditional video surveillance. The argument takes the initial analytical step of positing that existing precedent does not authorize the use of video analytics, with arguments pointing in the direction of finding a Fourth Amendment violation.

The second subpart builds on this argument, asserting that video analytics powered by AI-enhanced pattern matching – properly understood – is an overbroad, generalized search under the Fourth Amendment.[208] The argument explains that by design, video analytics technology cannot escape automated, large-scale, warrantless searching, matching, and tracking people and effects in ways that reveal the "privacies of life."[209] 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 violate a reasonable expectation of privacy (as least when applied to city-wide 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 concerns. As will be discussed, whether courts adopt either version or avoid the Fourth Amendment altogether, the constitutional issues present an existential question for the future of video analytics technology.

A. Video Analytics as a Search: Step One: "Digital is Different"

This section sets up a two-part argument about video analytics and "reasonable expectations of privacy." It concludes that the constitutional question remains open, not compelled by traditional "privacy in public" cases,[210] but that newer cases suggest a Fourth Amendment violation.

This provides authorities the power to index and search a vast database of objects, behaviors, and anomalous activity.").

[207] *See infra* Part III.A.

[208] *See infra* Part III.B.

[209] *Carpenter*, 138 S. Ct. at 2214 ("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))).

[210] *See supra* section II.B.

Part one sets the stage, arguing that video analytics should not be confused with traditional video surveillance but approached on its own terms. Part 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. Any court tasked with analyzing the Fourth Amendment considerations of video capture, needs to be clear whether they are examining traditional video surveillance or video analytics AI.

For judges, the most compelling reason for this distinction is that the law governing traditional video surveillance is already well settled.[211] 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.[212] 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.[213] It is hard to

[211] 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 areas frequented by a large number of people 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.").

[212] As discussed in Part II, case law from the 1960s-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*, 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*, 92 Haw. 454, 467, 992 P.2d 723, 736 (Ct. App. 1999) ("[T]he videotaping was of a public street with unlimited access and, therefore, Defendant's presence and/or transaction was "in a public place subject to public viewing or hearing." ... 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, 2012 270 P.3d 64, 70 (Mont. 2012) (Nelson, J. concurring) ("Montanans expect that they have a right of privacy in their affairs, even when they leave their homes—albeit, not to the same degree as they expect within their homes. We accept fixed cameras in various locations, like banks, parking garages, and businesses. We are willing to give up some privacy for the sake of the security that these devices provide. But we do not accept 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.").

[213] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("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, 455 (2018) (confirming this understanding that traditional cameras fall outside of Carpenter's holding).

read *Carpenter* as altering existing law around traditional security cameras.[214]

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 networked *video analytics* system violates a reasonable expectation of privacy. Maybe it does, maybe it does not, but the reason why is not because courts unthinking 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, but 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.[215]

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 city-wide system for similar matches of that particular red shirt and the red shirted man (and other men wearing red shirts and all other

---

[214] Cases after *Carpenter* suggest there is little change to analysis about traditional video surveillance. *See e.g.*, *Commonwealth v. Mora*, 485 Mass. 360, 369, 150 N.E.3d 297, 307 (2020) ("The United States Supreme Court recognized this traditional nontargeted use of video cameras when it referred to "security cameras" as among the "conventional surveillance techniques and tools" that were not called into question by its holding in Carpenter. … Law enforcement officers appropriately have relied on security cameras, and other forms of nontargeted video surveillance, to identify and apprehend suspects."); *People v. Destefano*, 74 Misc. 3d 858, 866–67, 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, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 n.106 (2002) (listing cases).

[215] While there is an open question about the aggregation of these images or the tracking capabilities of city-wide 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* note xx.

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 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).[216] Inherent in the program are multiple (really continuous) searches of past collected data, comparisons, analysis, and visualizations – all without the officer doing anything but turn on the system.

Whatever one makes the above 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 watching the man in the red shirt above is one of monitoring and then investigation, but the same result can be seen in pre-programming the search for men in red shirts automatically. The video analytics system is doing the same thing of digitizing every object, and that thing 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.

[216] Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. 2007, 2026 (2022) (describing data and algorithmic errors in the criminal legal system).

2. The Underlying Logic of No Privacy in Public Does Not Fit Video Analytics

This second subpart 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 knowing and voluntary exposure to public observation essentially forfeits a claim to privacy.[217] Second, it is argued that because a human police officer could watch the person on the street without it violating an expectation of privacy, then a camera doing the same thing does not change the expectation.[218] Third, it is argued that in public there is nothing private or intimate being revealed beyond what any other person could see.[219] In other words, in public, one expects to be seen by other humans, and thus 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 in public. Those are different capabilities and arguing that you have no expectation of privacy of being seen in public, does not mean that you do not have an expectation of privacy from those other tracking, sorting, and storing capabilities.[220] 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 and does not signify that you are forfeiting other rights.[221]

---

[217] *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.") (citing Katz). *See* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) (discussing knowing disclosures and the Fourth Amendment).

[218] *See e.g.*, *Vega-Rodriguez v. Puerto Rico Tel. Co.*, 110 F.3d 174, 181 (1st Cir. 1997) ("[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.").

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

[220] Nor is it an issue of consent. Leaving one's home does not entail a consent for whatever might happen to you. *See generally* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U.L. REV. 1461, 1464 (2019).

[221] *See generally* Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 190 (2008) (discussing the concept of spatial privacy and how the law shapes expectations).

Second, as discussed in Part II, the Fourth Amendment doctrine around expectations of privacy has been largely controlled by human observations.[222] The overflight cases (*Ciraolo* and *Riley*) both were expressly limited to human observation, even though mechanical transportation was involved.[223] The beeper cases (*Knotts and Karo*) also turned on the limits of human tracking capabilities even though a wireless beeper was used.[224] The Supreme Court relied on an analogy to human observations as the limiting factor for finding no reasonable expectation of privacy in public.[225] 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.[226] 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.[227] Video analytics offer decidedly non-human capabilities, giving police departments superhuman powers to see everything, and catalog everyone.[228] Measured against expectations of privacy from human observers, video analytics is far more powerful and revealing. The system is "qualitatively different."[229] Again, while there is

---

[222] The one exception to this rule is the Supreme Court's decision in *Dow Chem. Co. v. United States*, 476 U.S. 227, 229 (1986), involving surveillance of an industrial plant for environmental protection investigation reasons. In Dow, the Court allowed for powerful camera surveillance. *See id.* at 228 ("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."). 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*, *see* Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 830 (2022).

[223] *Ciraolo*, 476 U.S. at 213; Riley, 488 U.S. at 448.

[224] *Knotts.* 460 U.S. at 285

[225] *Id.* at 282 ("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 also on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation.").

[226] Kyllo v. United States, 533 U.S. 27, 34, 40 (2001) ("To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.").

[227] *See supra* notes xx, xx.

[228] Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 31–32 (2022) ("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.").

[229] This is the term from *Riley* and *Carpenter*. *See Riley*, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)); see also *Carpenter*, 138 S. Ct. at 2214.

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

Finally, 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 short term 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.[230]

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 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, 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 also inexact, as the patterns are saved and searchable for weeks or months. 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 harm is systemic, not episodic.[231]

Or perhaps, one could argue that algorithmic nature of the anomaly alert reduces the privacy harm. After all, at some level of abstraction, the fact that computer vision can only recognize an object via pixels, militates against a clear individualized privacy harm. Remember, the object being identified in video analytics is a pattern-matched object that matches the object in the frame. If you think about the object being identified as not as "John Roberts" but a collection of pixels that represent a man wearing a red shirt and pants, similar to other images stored with the same pixels, the level of privacy exposure is less. Even if the system automatically captures the pixels that represent "John Roberts" as he goes about his business, picks up his kids, goes to a bakery, takes a walk in the neighborhood, the system is just

[230] *See supra* notes xx, xx, discussing *Carpenter* and the *Jones* concurrences.

[231] In a prior article, I address how similar systems of surveillance like the persistent surveillance planes like those that flew over Baltimore and long-term pole cameras create similar systemic harms. Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 48 (2022).

recognizing pixels. At this level of abstraction, the reveal of the pixels feels less privacy invasive, even though it would be trivially easy for a police officer to connect the dots of the human object who is that collection of pixels.

If you have just read the above paragraphs and concluded that video analytics are a bit more complicated than you thought, and you are unsure of how you feel about AI-powered computers pattern matching the pixels of John Roberts as he goes about his 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 the computer vision is creating object recognition pattern matching on our lives, and thus doing so would be an unreasonable expectation. It would seem a stretch to claim that "John Roberts" objectively and reasonably expects (or has voluntarily agreed) that his pixels will be identified in a network of cameras stretched across a city and that society thinks such an expectation is reasonable.[232]

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 with video analytics and not blindly apply video surveillance precedent to a very different privacy problem.

B. Video Analytics as a Search: Step Two

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.[233]

The first step of my argument merely claims that courts should not apply old precedent to a new problem, because the technology and privacy issues are just too different.[234] The second step of my argument goes further explaining that automated, AI-enhanced video analytics is a Fourth Amendment search. Further, use of video analytics is likely an unconstitutional search because no warrant can be obtained before the

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

[233] *See generally*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1128 (2021) (discussing facial recognition); Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 53 (2020) (discussing smart cities).

[234] *See also* Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 853 (2022) (detailing how archaic many of the technologies were that still serve as precedent in modern cases).

generalized pattern matching occurs in a system of continuous surveillance (and no exception applies).[235] Whether we are talking about investigation, virtual patrols, or anomaly alerts, the city-wide matching 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 of networked cameras, this exposure violates a reasonable expectation of privacy and thus the Fourth Amendment.

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 (public movements) from digital tracking technologies – even in public.[236] Second, those cases highlight a concern with systems of data collection that are arbitrary, aggregating, permeating, and allow generalized retrospective queries.[237] At some moment along a (still unsettled) continuum, the Supreme Court has found police surveillance powers to violate a reasonable expectation of privacy.[238] Both doctrinal clues about (1) tracking movements in public and (2) surveillance systems are helpful to answer the video analytics search question. Both point toward the claim that such 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 in 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 –

---

[235] *See infra* Part III.C

[236] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (discussing the "tracking capacity" of CSLI); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (discussing tracking as a search).

[237] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1129-41 (2021) (discussing these principles as part of how the Court can "future-proof" the Fourth Amendment).

[238] Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 80 (2020) (describing a similar continuum analysis).

even in public spaces.[239] 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.[240] Timothy Carpenter was tracked from store to store by his cellphone.[241] 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 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.[242] The *Carpenter* Court could have analogized to *Knotts* to argue that Timothy Carpenter had knowingly exposed his location by being in public.[243] The Court also could have analogized to *Miller* or *Smith* (the third-party records cases) to argue that he had voluntarily revealed his location data to a third party cellphone provider.[244] Instead, the Court found (long-term) location data to be constitutionally protected because society does not expect to be publicly tracked by the police.

Video analytics through Real-Time Crime Centers offers a more revealing digital tracking power than either GPS or CSLI. With video analytics, police get location, time, but also content of what the person is doing in public. Whereas with GPS and CSLI, police needed 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.[245] Such collection is within the default collection times for video analytics systems, as the systems are programed to collect and save information for weeks or

---

[239] *See infra* note xx.

[240] Jones, 565 U.S. at 403.

[241] Carpenter, 138 S. Ct. at 2212

[242] Jones, 565 U.S. at 429 (Alito, J. concurring) ("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.").

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

[244] *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.").

[245] *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, 428-30 (Alito, J., concurring in the judgment) (mentioning "long-term tracking").

months.[246]

Before moving on, this last point about the scale and scope of data collection 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 though collected data.[247] With an appropriate search query, police can locate the man with the red shirt in the camera data over the last days, weeks, etc. Like CSLI, object location can be mapped over time. Whether it is seven days or 28 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 pre-programmed into the system, the analytics program is still automatically tracking movements and identifying people in public for long periods of time behind the scenes. Just because a government agent is not actively sorting through the data, it does not mean that government 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, pre-programmed, 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. Whether the police officer actively queries the system, passively watches it, or lets a pre-programmed algorithm search, the same system-wide, 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.

---

[246] *See* Zac Larkman, *The Quiet Rise of Real-Time-Crime Centers*, WIRED (July 28, 2023) https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/ (discussing data retention practices).

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

b. Systems of Surveillance

Public tracking was the act in *Carpenter* and *Jones*. That is what the police did: they tracked a suspect. But the Supreme Court was equally concerned with unregulated *systems* of surveillance that granted police the power to investigate everyone or anyone for any reason.

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 a vast dataset 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.[248] In addition, both GPS and CSLI technologies allowed police to aggregate different data points with other information revealing personal details about a life.[249] 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[250] and revealing "the privacies of life."[251] Combining these concerns together, the Supreme Court drew the line at digital technologies that were too permeating and arbitrary and that allowed for comprehensive, retrospective, and aggregating details of personal lives and associational connections.[252] 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

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

[249] *Jones*, 565 U.S. at 416 (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."); Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579 (2017) ("I contend that when 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.").

[250] *See supra* note xx.

[251] *See supra* note xx.

[252] 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 (2022); Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 13 (2020); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 359 (2019).

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.[253] The Fourth Amendment framework shows how the Supreme Court has drawn the line against certain future threats from digital surveillance systems.[254] 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 raise related privacy concerns. First, as discussed, the systems are *tracking* technologies that reveal movements and patterns in physical space.[255] Second, the technologies are *too permeating* in nature, making data capture difficult to avoid.[256] 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.[257] Fourth, the data collected is *retrospectively* searchable, allowing for indiscriminate and indeterminate searches into the information.[258] Fifth, the collected data can

---

[253] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1129-41 (2021) (detailing the "future-proofing" principles).; Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 53 (2020); Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 Ala. L. Rev. 1, 48 (2022).

[254] *Id*.

[255] *See supra* note xx (discussing tracking). Nirja Chokshi, *How Surveillance Cameras Could be Weaponized with AI*, NY TIMES (June 18, 2019) ("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.").

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

[257] A concern with arbitrary policing power is central to Fourth Amendment theory. *See Carpenter*, 138 S. Ct. at 2213 ("[t]he '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.'"); *see also id*. at 2213-14 ("Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "*arbitrary* power."); *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.").

[258] *Carpenter*, 138 S. Ct. at 2218 ("[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."); *see also* Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 951 (2016) (discussing the danger of giving police a "time-machine" to go back to investigate anything they wish).

be *aggregated* to reveal personal details, patterns, or hidden connections that would not be connectable otherwise.[259] Sixth, the impact of these technologies undermines *associational freedoms*, religious activity, dissent, personal choice, and infringes other constitutional rights.[260] Finally, the technologies provide a qualitatively different *superpower* that makes the technology more than a human enhancement from an analog era.[261] 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.[262] 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.

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.

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

[259] Both *Jones* and *Carpenter* discuss the privacy harms from aggregating different pieces of personal data. United States v. Jones, 565 U.S. 400, 413–16 (2012) (Sotomayor, J., concurring); *id*. at 429–31 (Alito, J., concurring). *See also* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1834 (2014) (describing the mosaic theory and its privacy harms).

[260] *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.").

[261] Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the Carpenter Decision*, 16 OHIO ST. 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.").

[262] *See supra* note xx.

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. 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 to identify criminal associates, but also can be used to investigate First 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, 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 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 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 and monitoring. While the object recognition technology behind anomaly alerts is the same as the technology powering investigation and monitoring, in application there are different privacy impacts.

For example, if a computer alerts to the presence of an individual in a parking lot when ordinarily there is 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 pre-programmed 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. A preprogrammed alert 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 include other information about other times. Finally, the pre-programmed nature of the suspicion seems less arbitrary and pervasive as it has been pre-planned and essentially suspicionless.[263] The result is that there is less private information revealed or even potentially revealed in an anomaly alert and less concern about police discretion and abuses.[264]

Applying the future proofing principles to anomaly alerts confirms these different privacy impacts. For example, anomaly alerts (bag detection, unusual movements) are not primarily *tracking* technologies. They identify

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

[264] There are other reasons to object to anomaly detection outside the Fourth Amendment context. Predictive suspicion systems raise real concerns with error, bias, and equity (in investigation and at trial). The preprogrammed suspicious prompts are developed outside the policing context by private developers, and might not take into account issues of economic, social, or racial differences. 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. Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2007 (2017).

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 pre-set criteria have been designed in advance. In addition, the pre-programmed nature of the alert distinguishes the alert from retrospective searches into past data and makes *aggregation* of personal data difficult. Of course, these systems can still chill *associational* freedoms[265] and do offer a *superpower* beyond any human capability, but the privacy impacts are different.

Even acknowledging the difference with anomaly alerts, we run to 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 surveilles 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 tracks 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.[266] The question for judges is which one is the proper focus.

In prior work, I have called this distinction "the unit of surveillance question"[267] and it likely would shape any 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*. 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,

---

[265] 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.

[266] 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. The traditional canon cases focused on the result of that collection.

[267] Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 4 (2022) (discussing the term).

suggesting that the Court cared more about the potential investigatory power given to police using CSLI than the actual use of that power. The Court explicitly warned about a power that could uncover data about anyone for any reason.[268] 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 real privacy interests. 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.[269] 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 privacy harm of whether Antoine Jones was near a particular narcotics stash house or not.[270]

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 negligible 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 city-wide 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.[271] The same logic should hold for police

[268] Carpenter, 138 S. Ct. 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.").

[269] *Id*.

[270] *Jones*, 565 U.S. at 416 (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, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society.").

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

wanting to query video analytics data. If the use of video analytics is a Fourth Amendment search, then a warrant (or exception) is required.[272] In practical terms, to find the robbery suspect in the red shirt from the collected video streams digitally sorted by objects 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 collection, but to locate that particular red shirt, police already had to have collected images of everyone wearing a red shirt.[273] By design, the 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.[274]

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.[275] 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.[276] In both cases, the question would not be whether a warrant could be obtained, but whether this initial act – independent of the

---

[272] 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. The *en banc* court concluded that such systemic city-wide surveillance violated a reasonable expectation of privacy. 2 F.4th 330 (4th Cir. 2021).

[273] 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).

[274] The debate about Fourth Amendment collection and use restrictions has been an ongoing one. *See generally* Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 138 (2017); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 4-5 (2015).

[275] 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 any car including the Justices' cars. Transcript of Oral Argument at 9, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), available at http://www.supremecourt.gov/oral_ arguments/argument_transcripts/10-1259.pdf.

[276] One need not imagine too much, because police have contracted with a company called Fog Reveal that provides geolocational data to police as a paid service. Police can use geolocation coordinates (like CSLI and GPS) to track any smartphone by simply querying a dataset created by the company for law enforcement. To work as a retrospective search, the system must collect and retain the locational data, thus created 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; Will Greenberg, *Fog Revealed, A Guided Tour of How Cops Can Browse your Location Data*, EFF https://www.eff.org/deeplinks/2022/08/fog-revealed-guided-tour-how-cops-can-browse-your-location-data.

later warrant – would have violated the Fourth Amendment. Both *Jones* and *Carpenter* suggest that these acts would violate a reasonable expectation of privacy. To be fair, these were not the factual circumstances in *Jones* or *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.[277]

Similarly, and perhaps more intuitively obvious, police cannot obtain a warrant for video analytics-enhanced virtual patrols. 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.

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.[278] 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 particularized use of police power based on individualized probable cause. 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 would choose

---

[277] Andrew Guthrie Ferguson, Digital Rummaging (forthcoming Wash. U. L. Rev. 2024).

[278] *United States v. Grubbs*, 547 U.S. 90, 96–97 (2006) ("Anticipatory warrants [] require the 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.); *see also Fourth Amendment - Anticipatory Warrants*, 120 HARV. L. REV. 154 (2006) (describing the limited nature of anticipatory warrants).

to analyze the problem outside the somewhat ill-fitting "reasonable expectation of privacy" threshold 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.[279] 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 of the decisions are governed by pre-programmed algorithms. Just as a matter of doctrinal fit, the timing of when the "search" was programmed, and the automatic nature of the pattern matching does take the question out of the usual human police officer situation (and the usual fear of human police officer discretion).[280]

First, as to the pre-programming argument. Pre-programming 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 pre-programmed a computer program to hack my WiFi 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 pre-programing the intrusion for some time in the future. Similarly, it seems appropriate to hold police to account for the algorithmic systems they buy and deploy in cities.[281] 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.[282]

In addition, courts should recognize the cost in exempting algorithms

---

[279] Police must ultimately be responsible for the choices they make to buy certain technologies. *See generally* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1595 (2016) Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. Rev. Online 19, 20 (2017).

[280] Christopher Slobogin, *Suspectless Searches*, 83 OHIO ST. L.J. 953, 958 (2022) (discussing searches that are more administrative in nature).

[281] *See generally* Renata M. O'Donnell, *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, 94 N.Y.U. L. REV. 544, 576 (2019) (making an argument why police should be held responsible for algorithms that create racial disparities).

[282] 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 TECHNOLOGY (2018); Matt Stroud, THIN BLUE LIE: THE FAILURE OF HIGH-TECH POLICING (2019).

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.[283] Put another way, the pre-programmed 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 friend, 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[284] (more civil rather than criminal). Doctrines like the "community caretaker" exception do allow police to search for non-criminal purposes, but establishing a city-wide surveillance system to do the same thing seems an expansion beyond the narrowly crafted warrant exception.

The problem with this community caretaker argument is twofold. First, police in a 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.[285]

---

[283] *See supra* notes xx.

[284] 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*, 547 U.S. 398, 400 (2006) the Court found entry into a house to prevent injury from a fight to be reasonable. What had been known as the "community caretaker" exception from *Cady v. Dombrowski*, 413 U.S. 433 (1973) has recently been narrowed in *Caniglia v. Strom*, 593 U.S. 194, 196 (2021) in which the Court limited non-emergency warrantless entries in a home on a community caretaking theory.

[285] The focus of the Real-Time Crime Center is investigating crime. *See e.g.,* Michael Gallensberger, *Garry Police Department Unveils Real Time Crime Center*, Lakeshore Public Media (Nov. 21, 2023) (quoting Corporal Larry McKinley who oversees the crime center, "[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"). https://www.lakeshorepublicmedia.org/local-news/2023-11-21/gary-police-department-unveils-real-time-crime-center; Bria Bolden, *How 'Connect 2 Memphis' works: A Look Inside MPD's Real Time Crime Center*, Action News 5 Memphis (Dec. 18, 2023) ("People are skeptical because they think 'Big Brother' is watching," said Deputy Chief Joe Oakley. "That's not what we're doing. We developed this program to help our city stay safe and reduce our crime numbers.")

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.[286] 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 clearly, police 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. Also, just a doctrinal matter, the narrow community caretaker exception would need to be radically rewritten to incorporate the routine captured by a real time crime center.[287]

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.[288] The Fourth Amendment is not only concerned with threshold search questions. Reasonableness has also been a way to address arbitrary or overbroad police actions.[289] 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 for Fourth Amendment purposes.[290] That said, when it comes to programmatic

---

https://www.actionnews5.com/2023/12/19/how-connect-2-memphis-works-look-inside-mpds-real-time-crime-center/.

[286] *See generally* Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION 143-84 (2017) (discussing how generalized suspicion distorts Fourth Amendment doctrine around probable cause and individualized suspicion).

[287] The Supreme Courts most recent foray into the subject suggests that the Court will keep the exception narrow. *See Caniglia v. Strom*, 593 U.S. 194, 196 (2021).

[288] Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is "reasonableness"); Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 978 (2004) (discussing the history of reasonableness from the Founding Era on).

[289] *See, 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.").

[290] 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) ("The concern with general warrants and writs of assistance thus forms a rich historical backdrop to the Fourth Amendment's development and has continued to play an important role in shaping the ongoing debate over whether the "reasonableness" or the "warrant" clause should have primacy in interpreting how the Fourth Amendment should be applied. … Although the Court recently has given increasing credence to the reasonableness approach, the Court through most of the twentieth-century has used a warrant-preference approach and has relied upon the idea that the Framers preferred specific warrants because it curtailed the discretion of law enforcement agents to act without judicial approval.").

surveillance systems – like video analytics in all its forms – the reasonableness argument offers a way forward.[291]

A reasonableness argument would look at a system of video surveillance and ask whether such a public safety system is reasonable.[292] The analysis is akin to special needs searches[293] and the balancing test that the Supreme Court has undertaken in other circumstances.[294] 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).[295] 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.[296] So, for example, security to get into the Superbowl might require 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.

A city-wide video analytics system is not analogous to the Super Bowl analogy, but in essence the argument would be that city-wide video analytics is not being used for law enforcement investigation, but for public safety reasons more broadly. Under this argument, the benefit of increased

---

[291] *See generally* Christopher Slobogin, VIRTUAL SEARCHES: REGULATING THE COVERT WORLD OF TECHNOLOGICAL POLICING (2022).

[292] Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 90-118 (2007). *See also* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 n. 106 (2002); *see also* Zeus Kerravala, *Fact of Fallacy: Video Cameras Are More than Just Another Set of Eyes*, STATE TECH MAGAZINE (July 24, 2023) ("[V]ideo surveillance is a multipurpose public safety technology that's not only used for crime reduction. There are several other practical applications that include event monitoring, traffic control and enforcement, and hazmat response. Surveillance is used to keep an eye on crowded public events such as political rallies and sports games.").

[293] 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.").

[294] *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, 169 (2020) (describing the history of reasonableness balancing).

[295] John J. Miller et. al., *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).

[296] *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."' (internal quotations and citations omitted)).

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 quite substantial.[297] In addition, the efficacy argument is confused, 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.[298] Police are using the cameras to scan everywhere the cameras point 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.[299]

In addition to being general (in that video analytics collects too much), the pattern matching predictions are also not particularized.[300] Here

---

[297] *The Technology that Powers Real Time Crime Centers*, POLICEONE (Sept. 27, 2023) https://www.policemag.com/technology/article/15635270/how-technology-powers-real-time-crime-centers ("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. The core function of an RTCC is data gathering, analysis, and sharing information to aid in decision making and response coordination.").

[298] Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 727 (2018) ("[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. This latter protection undergirds the Fourth Amendment's prohibition against general warrants and other suspicionless programs designed to "detect evidence of ordinary criminal wrongdoing.").

[299] *See generally* 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 in part because officers were authorized to search and seize upon bare suspicion. They were also arbitrary and dangerous because agents of the executive were given 'unlimited discretion' to choose whom, where, and what to search and seize." (footnotes omitted)); 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.").

[300] 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 it is impossible to particularly describe the place to be searched because the place may be

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.[301] 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.[302] The pre-programmed objects or anomalies may be based on hunches, biases, or theories having no scientific basis that some collection of pixels is suspicious or not.[303] And when used, by definition, the predicted anomalies have nothing to do with the individual person being alerted to.[304] 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 would 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 the question of reasonable expectations of privacy from city-wide 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 systems like BriefCam or similar video analytics

---

every place the target goes over the course of a month?").

[301] 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. 151, 160 (2021) ("Understanding race and technology as both inherently social phenomena encourages a more critical eye that denounces the assumed objectivity of a tool.").

[302] 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.").

[303] Nirja Chokshi, *How Surveillance Cameras Could be Weaponized with AI*, NY TIMES (June 18, 2019) ("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.").

[304] 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).

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 of current 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, and cases that relate only to police tools are unhelpful precedent. The continuous nature of collection, the temporal distortions of retrospective access, the pre-programed predictive alerts, and the ability to track through time, all upend traditional Fourth Amendment doctrine. The application of the Fourth Amendment to video analytics presents a helpful test case to determine how a reimagined Fourth Amendment might protect against new privacy threats, but also leaves many open questions.

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 to 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 city-wide video analytics systems.