

Piecing Together Privacy: AI-Enhanced Surveillance, the Fourth Amendment and the Mosaic Theory^{*}

Lauren Welter[†] and Grace Van Meter[‡]

Abstract

This article examines the constitutional implications of artificial intelligence (AI) in law enforcement surveillance in the context of the Fourth Amendment. Facial recognition, predictive policing, and automated license plate readers may enhance investigative efficiency, but this article examines how it may also pose significant privacy risks. Drawing on key precedents (Katz, Jones, Carpenter) as well as the Mosaic Theory, this article evaluates how aggregated data changes the field of traditional search analysis. This article further challenges existing frameworks, including the Stored Communications Act and Executive Order 14110, and identifies regulatory gaps. This article highlights the need for transparency, robust warrant requirements, and independent oversight. Finally, this article advocates for a legal framework that utilizes technological innovation without sacrificing constitutional protections.

A Introduction

The rapid advancement of artificial intelligence (AI) technologies has revolutionized surveillance capabilities, raising critical questions about their compatibility with the Fourth Amendment's protections against unreasonable searches and seizures. As AI-driven tools such as facial recognition, predictive policing and automated licence plate recognition (LPR) become increasingly prevalent, they offer unprecedented efficiency and accuracy in law enforcement. However, these technologies also pose significant risks to privacy and civil liberties, potentially enabling pervasive surveillance without adequate oversight or accountability. This article examines the intersection of emerging AI technologies and Fourth Amendment jurisprudence, arguing for a nuanced legal framework that safeguards individual rights while embracing technological innovation.¹

^{*} With help from AI.

[†] Lauren Welter, Editor-in-Chief, Indiana International and Comparative Law Review, Vol. XXXV. J.D. IU McKinney School of Law 2025.

[‡] Grace Van Meter, J.D, Indiana University Robert H. McKinney School of Law 2025. B.A., Indiana University Bloomington (2021).

¹ AI generated using Microsoft Copilot.

Or so Microsoft Copilot, an AI-powered chat service, states when given the prompt: “Please suggest a good opening statement regarding how emerging AI is important to consider in the context of the Fourth Amendment for a law review article?” AI assistants and chatbots are likely the most well-known forms of AI known to the public at this time, with ChatGPT receiving around 200 million weekly users as of August 2024.² However, as Copilot so eloquently put it, AI is also being utilized in other important sectors that affect everyday life, including surveillance.

While the use of AI in conjunction with policing practices may, as some argue, improve policing capabilities, it also brings forward Fourth Amendment and privacy concerns. Under the Fourth Amendment, people are protected from arbitrary searches and seizures, requiring police officers to get warrants based on probable cause. The legal safeguards created by the Fourth Amendment are challenged by the use of AI-driven surveillance tools like the ones Copilot referenced. The contemporary legal framework, including seminal court cases that further shaped the scope of Fourth Amendment protections, must evolve with the complexities of introducing AI into surveillance and traditional policing practices. Finding a balance between utilizing AI’s advantages for improved police and protecting constitutional rights is crucial as the technology develops. This article aims to analyse the legal, ethical and societal implications of AI integration into policing practices and how courts should consider Fourth Amendment issues considering these recent developments.

I AI: Generally, and Its Use by Law Enforcement

Understanding AI is incredibly difficult but it is even more challenging to simplify its complex components and subparts into something that can be considered a baseline knowledge. However, this basic understanding of AI is crucial to recognizing its current use by law enforcement, the potential it has and the threat its potential poses to civil liberties.

Often the term artificial intelligence or its acronym, AI, is utilized as a buzzword to invoke fear of a future of government overbearance and technological takeover, but much of this anxiety of technological advancement stems from a misunderstanding of AI.

First, AI is not a new and emerging phenomenon and has existed, and continues to, in the daily lives of many without recognition. AI in the United States has been developing for at least fifty years,³ and new AI tools are mere advancements of an already existing technological concept.

In August 1955, a group of four individuals including at Dartmouth College proposed a summer research project on ‘artificial intelligence’.⁴ One of the four was

2 *OpenAI Says ChatGPT’s Weekly Users Have Grown to 200 Million*, Reuters (29 August 2024, 5:40 p.m.), <https://www.reuters.com/technology/artificial-intelligence/openai-says-chatgpts-weekly-users-have-grown-200-million-2024-08-29/>.

3 R. Cordeschi, ‘AI Turns Fifty: Revisiting Its Origins’, *Applied Artificial Intelligence*, Vol. 21, 2007, pp. 259-279. <https://doi.org/10.1080/08839510701252304>.

4 J. McCarthy, M.L. Minsky, N. Rochester & C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth (31 August 1955), <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>. <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

the computer scientist and Dartmouth assistant professor John McCarthy, credited with coining the term ‘artificial intelligence’ in the proposal that preceded the conference.⁵ McCarthy has defined AI as “the science and engineering of making intelligent machines” and recognized the existence of AI well before the 1956 Dartmouth Summer Research Project on Artificial Intelligence.⁶

Alan Turing, an English mathematician and the creator of the Turing Test, was one of the first to work with “intelligent machines”, according to McCarthy.⁷ Turing worked with machines beginning in the 1930s and developed the Turing Test in 1950, when he proposed in an article a way to determine whether machines are “intelligent”.⁸ The Turing Test tests whether a human can engage blindly with both a machine and a human without being able to distinguish between the two.⁹ This test is both widely respected and criticized today, with McCarthy describing it as “a one-sided test”.¹⁰ McCarthy argues that a machine that passes the test is certainly intelligent, but a machine could still be intelligent without being able to pass the test.¹¹ Yet, the Turing Test remains one of the few methods for gauging the intelligence of a machine.

This leads to the second point: the lack of a definitive explanation for machine ‘intelligence’ means that AI itself is essentially undefined, which in turn creates confusion as to what AI is. McCarthy himself has admitted that there are no real guidelines or determinations of what actions are considered ‘intelligent’ for machines and no definition of intelligence exists outside the one that relates to human intelligence.¹² His personal definition of intelligence was “the computation part of the ability to achieve goals in the world” and is observed in “varying kinds and degrees” in people, animals and some machines.¹³ If this definition seems vague and ambiguous, it is because it is. And because the concept of ‘intelligence’ in machines is so vague and undeveloped, AI itself lacks a widely adopted definition.

Over time, people have recognized AI to be less of a thing and more of an overarching category or concept, encompassing many subparts – subparts such as ‘machine learning’, which is the use of historical data and algorithms in training AI systems to make predictions or decisions.¹⁴ Beyond “machine learning” is its subset “deep learning”, which works to imitate the human brain in its ability to make decisions.¹⁵ All of these buzzwords fall underneath the umbrella of AI, but to avoid diving further into the endless complexities of what

5 John McCarthy, *What Is Artificial Intelligence?* Stanford (12 November 2007), <https://www-formal.stanford.edu/jmc/whatisai.pdf>.

6 *Ibid.*

7 *Ibid.*

8 *Artificial Intelligence: Everything You Need to Know Magazine* (2023) – From Our Canvas Page.

9 Alan M. Turing, ‘Computing Machinery and Intelligence’, *Mind*, Vol. 49, 1950, pp. 433-460. <https://courses.cs.umbc.edu/471/papers/turing.pdf>.

10 McCarthy, *supra* note 5.

11 *Ibid.*

12 *Ibid.*

13 *Ibid.*

14 Cole Stryker & Eda Kavlakoglu, *What Is Artificial Intelligence?*, IBM (9 August 2024), <https://www.ibm.com/think/topics/artificial-intelligence>.

15 *Ibid.*

AI includes and what it is, it is easiest to just demonstrate everyday use of AI as an example of the myriad ways AI is utilized.

B AI in Everyday Life

The first example of AI most people think of is chatbots such as ChatGPT and Google Gemini. Chatbots are AI that utilize machine learning based on other conversations to engage in text conversations.¹⁶ However, people forget that there have been other examples of AI ingrained in daily life even before ChatGPT existed, such as digital assistants.

Digital assistants include Siri, released by Apple in October 2011 as a new iPhone feature, over a decade ago.¹⁷ An estimated 53% of smartphone sales in the US are of iPhones, and globally there are an estimated 1.382 billion iPhone users.¹⁸ This means a lot of people utilize AI daily when they ask Siri what the weather is, what time a store closes or to place a phone call hands free. Alexa, which is a component and primary feature of Amazon devices such as the Echo, was announced in 2014.¹⁹ This device, which is considered just an alarm or music speaker by many, is in fact an example of AI. The oversight in acknowledging that AI is already integrated into daily life through devices like these arises from not realizing that the use of AI is deeply embedded in technological progress. Virtually all new technologies developed since the term ‘artificial intelligence’ was coined have relied on AI to some extent.

III Law Enforcement Use of AI

Law enforcement utilizes AI in a multitude of ways, some of which will be discussed in this article in depth. However, the law has only begun to address AI use by law enforcement as it presents new legal issues.

In November 2024, the International Association of Chief of Police (IACP) held their annual conference in Boston, Massachusetts, where AI was a major focus of the conference.²⁰ IACP is the largest assembly of police chiefs in the US, providing a venue for officers to engage in discussions, showcase and demo products and receive recognition through awards.²¹ The AI portions of the conference focused on three key areas: virtual reality training for officers, automation of administrative tasks such as report writing and, most intriguing, integrated data collection and

16 *Use AI-Powered Chatbots to Deliver Automated Conversations*, Google Cloud, <https://cloud.google.com/use-cases/ai-chatbot> (accessed 19 December 2024).

17 Doug Gross, *Apple Introduces Siri, Web Freaks Out*, CNN Business (4 October 2011), <https://www.cnn.com/2011/10/04/tech/mobile/siri-iphone-4s-skynet/index.html>.

18 *iPhone Users and Sales Stats*, Backlinko (10 December 2024), <https://backlinko.com/iphone-users>.

19 Cadie Thompson, *Amazon Surprises with New Device: A Voice Assistant*, CNBC (6 November 2014), <https://www.cnbc.com/2014/11/06/amazon-surprises-with-new-device-a-voice-assistant.html>.

20 James O'Donnell, *How the Largest Gathering of US Police Chiefs Is Talking About AI*, MIT Technology Review (19 November 2024), <https://www.technologyreview.com/2024/11/19/1106979/how-the-largest-gathering-of-us-police-chiefs-is-talking-about-ai/>.

21 *Ibid.*

analysis.²² This includes various tools such as drones, licence plate readers and even gunshot detection tools.²³ Each year police chiefs across the US are being exposed to new ways to incorporate AI into their policing, and simultaneously, average citizens are becoming more aware of the implications of these technologies becoming standard in law enforcement practices.

1 Facial Recognition Technology

While facial recognition technology began to emerge in the 1960s, AI and machine learning are now being utilized in conjunction with these well-known techniques to more efficiently monitor crowds, find missing individuals and prevent or solve crimes.²⁴ According to Human Rights Watch, the use of AI to facilitate a broader use of facial recognition surveillance technology undermines international human rights law, privacy rights, freedom of expression, freedom from discrimination and more.²⁵ In actuality, at least with regard to the US, most Americans believe that utilizing facial recognition in conjunction with AI may benefit police as they search for missing persons and investigate crime. This finding comes with the caveat that there are “some notable differences among racial and ethnic groups on these issues”, finding that people of colour are generally more sceptical of this sort of technology in the hands of police, believing that it may be used to monitor neighbourhoods of colour disproportionately to predominantly White neighbourhoods.²⁶

Interestingly, a very recent occurrence has cast doubt on the effectiveness of AI surveillance in apprehending criminals. On 4 December 2024, the CEO of UnitedHealthCare was fatally shot outside a healthcare investor day held at Hilton hotel in New York.²⁷ For five days, the shooter evaded the police and not for a lack of surveillance technology or efforts.²⁸ Since 2011 the New York Police Department has had a dedicated surveillance unit named the Facial Identification Section, which utilizes facial recognition technology to solve crimes.²⁹ Yet, even with more than a decade of using facial surveillance, the specially trained police were unable

22 *Ibid.*

23 *Ibid.*

24 Lee Rainie et al., 2. *Public More Likely to See Facial Recognition by Police as Good, Rather Than Bad for Society*, PEW Research (17 March 2022), <https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/>.

25 Anna Bacciarelli, *Time to Ban Facial Recognition from Public Spaces and Borders*, Human Rights Watch (29 September 2023, 3:09 p.m.), <https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders>.

26 Rainie et al., *supra* note 24.

27 Megan Cerullo, *Brian Thompson, UnitedHealthcare CEO, Shot Dead in Manhattan*, CBS News (10 December 2024), <https://www.cbsnews.com/news/brian-thompson-unitedhealthcare-ceo-manhattan-shooting/>.

28 Noor Al-Sibai, *AI Completely Failed to Catch CEO Killer, with Cops Instead Relying on Random McDonald's Employee*, Futurism (10 December 2024, 3:08 p.m. EST), <https://futurism.com/the-byte/ai-fail-uhc-killer-luigi-mangione>.

29 Danielle Genovese, *AI Catching Killer of UnitedHealthcare CEO Brian Thompson*, Fox Business (6 December 2024, 6:00 a.m. EST), <https://www.foxbusiness.com/lifestyle/ai-catching-killer-unitedhealthcare-ceo-brian-thompson>.

to locate the shooter, until a Pennsylvania McDonald's employee called in to report a customer the employee suspected was the shooter.³⁰

This incident underscores a critical limitation of AI surveillance: despite the utilization of advanced technology like facial recognition, drones, K-9 units and even scuba divers, the suspect managed to leave New York undetected.³¹ And, after everything, it was a human who identified the shooter after social media rapidly circulated images of the suspect. This raises concerns that financially emphasizing expensive surveillance techniques over other methods of crime solving, just as utilizing social media, may not be the best use of taxpayer funds.

2 Predictive Policing

Another way AI is now being utilized in conjunction with surveillance technology is with predictive policing. Predictive policing, traditionally, is when law enforcement utilizes data, street intelligence and crime analysis with geospatial technologies and intervention models to predict when crime may occur, therefore reducing crime and improving overall public safety.³² While predictive policing used to mean that law enforcement was analysing the data on their own, AI has taken the grunt-work out of the analysis by using machine learning algorithms to analyse the data more quickly and accurately than individual officers.³³ However, some are concerned that this process in itself is problematic as the data used in teaching the machine learning models are inherently biased data.³⁴

One example of this bias is relatively straightforward: Black individuals are more likely than White individuals to be reported for a crime, and based on this data, the AI will mark Black neighbourhoods as being 'high risk', although the only marker for doing so is the race of the residents. As more law enforcement personnel are sent to these 'high risk' neighbourhoods, 'more' crime is likely to be reported, given that the police are in the area with the specific goal of seeking out crime to 'prevent'. In this way, AI will continuously run on circular logic: now that these predominantly Black, 'high risk' neighbourhoods are found to be producing 'more' crime, its own biases are reinforced, and the AI will continue to indicate that a stronger police presence is needed in the area.³⁵

3 Data Collection and Analysis (Project Maven)

In order to hasten the US military's deployment of AI, Project Maven was started in 2017.³⁶ The National Geospatial-Intelligence Agency named the initiative a programme of record in November 2023 after it made great progress in investigating

30 Al-Sibai, *supra* note 28.

31 *Ibid.*

32 *Overview of Predictive Policing*, Nat'l Institute of Justice (9 June 2014), <https://nij.ojp.gov/topics/articles/overview-predictive-policing>.

33 Hope Reese, *What Happens When Police Use AI to Predict and Prevent Crime?*, JSTOR Daily (23 February 2022), <https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/>.

34 *Ibid.*

35 *Ibid.*

36 Ireland Degges, *NGA's Project Maven Focused on 'Building Ai the Right Way,' Says Maven Office Director Rachael Martin*, Govconwire (25 March 2024), <https://www.govconwire.com/2024/03/ngas-project-maven-focused-on-building-ai-the-right-way-says-maven-office-director-rachael-martin/>.

new AI technologies.³⁷ The project, officially called the Algorithmic Warfare Cross Functional Team (AWCFT), is a Pentagon project that aims to use machine learning and data fusion to process data from many sources, identify potential targets, transmit human decisions to weapon systems and utilize drones to record hours of footage every mission, among other functions.³⁸ The AI in Project Maven is not meant to select a target in combat but instead complement the human operator, said Marine Corps Col. Drew Cukor, the chief of AWCFT.³⁹

One objective of Project Maven is to create and incorporate computer-vision algorithms required to assist military and civilian analysts burdened by the overwhelming amount of full-motion video data that the Department of Defense (DoD) gathers daily to support counterterrorism and counterinsurgency operations.⁴⁰ Project Maven is set to expand by turning enormous amounts of data into actionable intelligence and increasing the quality and speed of decision-making, given the vast amounts of data collected by the DoD.⁴¹

At the time of its inception, the contractor who would develop the algorithms for Project Maven was still up in the air. However, in 2018, it became public knowledge that Google was helping build AI for the drones that would be used by operations such as Project Maven.⁴² Many Google employees expressed horror at the idea that Google was helping build AI for warfare, and by April 2018, over 3,000 Google employees had signed a petition protecting the company's involvement in Project Maven.⁴³ This all came to a head in early 2019 when Google officially backed out of Project Maven because of negative public perception of the project, which may be attributed to the lack of transparency surrounding the project.⁴⁴ Despite Google's departure, recent fiscal 2025 budget documents show that Project Maven (now referred to simply as 'Maven') is still evolving, with the funding allotted to the project to "support algorithm development, data preparation, and integration experimentation to create joint DoD and [Intelligence Community] capabilities".⁴⁵

While Project Maven certainly implicates challenges and discussion involving AI in warfare, it also demonstrates how the aggregation of data by high-scale government projects could potentially infringe on Fourth Amendment protections

37 *Ibid.*

38 Kelsey D. Atherton, *Targeting the Future of the DoD's Controversial Project Maven Initiative*, C4ISRNET (27 July 2018), <https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/>.

39 *Ibid.*

40 Adam Frisk, *What Is Project Maven? The Pentagon AI Project Google Employees Want Out of*, Global News (5 April 2018, 10:55 a.m.), <https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/>.

41 Cheryl Pellerin, *Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges*, U.S. Department of Defense (27 October 2017), <https://www.defense.gov/News/News-Stories/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/>.

42 Atherton, *supra* note 38.

43 Frisk, *supra* note 40.

44 Billy Mitchell, *Google's Departure from Project Maven Was a 'Little Bit of a Canary in a Coal Mine'*, FEDSCOOP (5 November 2019), <https://fedscoop.com/google-project-maven-canary-coal-mine/>.

45 Brandi Vincent, *Fiscal 2025 Budget Docs Reveal How Project Maven Is Still Evolving*, DEFENSESCOOP (14 March 2024), <https://defensescoop.com/2024/03/14/project-maven-fiscal-2025-budget-still-evolving/>.

if the collected data is used to build detailed profiles without proper oversight or warrants. The controversy surrounding Google's involvement in Project Maven highlights concerns about transparency and the ethical implications of AI in surveillance. Ensuring that such projects comply with Fourth Amendment standards is crucial to maintaining public trust and protecting civil liberties. Where does the line between individual privacy, national security and large-scale data collection and processing using AI models merge with law enforcement investigations and the Fourth Amendment?

4 Drones and Body-worn Cameras (BWCs)

BWCs and drone surveillance are also areas of law enforcement practice that have been impacted by AI. Drones, AI and BWCs can all be used to better analyse police incidents. BWCs provide an essential first-person perspective of the crisis as it is developing on the ground, and drones provide an aerial perspective.⁴⁶ Drone and BWC integration with AI may increase the amount and calibre of useful evidence gathered. While BWCs record police officers' direct interactions and circumstances, drones can offer broad aerial views.⁴⁷ Furthermore, training efficacy can be increased when combined with virtual platforms, such as the metaverse for simulation. By offering dynamic, scenario-based training modules, AI can play a significant role in virtual training environments. It may give feedback and evaluate officers' performance in real time, improving training results and increasing efficacy.⁴⁸ Therefore, the integration of drones, AI and BWCs in counternarcotics operations, or law enforcement in general, has the potential to greatly improve policing capabilities.

5 LPR Technology

LPR uses AI technology to capture and analyse vehicle licence plates through the use of high-speed cameras and software that can detect licence plate characters. LPR systems are being employed for various purposes, including as a method of enforcing parking permits. Institutions such as Indiana University have implemented LPR to ensure compliance with parking regulations.⁴⁹ On the other hand, more serious uses exist such as the Department of Homeland Security's 'DeepVIEW' project, which focuses on improving LPR technologies' accuracy and integration with other security measures.⁵⁰ This advancement could substantially improve law

46 Amanda Davies & Ghaleb Krame, 'Integrating Body-Worn Cameras, Drones, and AI: A Framework for Enhancing Police Readiness and Response', *Policing: A Journal of Policy and Practice*, Vol. 17, No. 1, 2023, p. 7.

47 *Ibid.*

48 *Ibid.*, at 8.

49 *License Plate Recognition*, Indiana Univ. Parking Operations, <https://parking.indiana.edu/lpr/index.html> (accessed 20 December 2024).

50 U.S. Department of Homeland Security, *Automatic License Plate Recognition (ALPR) Technology Fact Sheet* (2021), https://www.dhs.gov/sites/default/files/publications/2021_st_alprfactsheet_20210105_final508.pdf.

enforcement's ability to rapidly identify vehicles, potentially transforming policing strategies and operations.

B The Fourth Amendment and AI Surveillance

I *Historical Context of the Fourth Amendment*

The Fourth Amendment provides the following:

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁵¹

In the context of AI surveillance in the US, the Fourth Amendment serves as a vital legal barrier, requiring that any governmental use of AI surveillance tools must be justified and reasonable, often necessitating a warrant based on probable cause.

Traditionally Fourth Amendment jurisprudence relied on a more literal interpretation of the Fourth Amendment, where searches were interpreted as requiring physical trespass as shown in *United States v. Jones*.⁵² However, in 1967 in *Katz v. United States*,⁵³ the Supreme Court moved away from a strict trespass only approach and adopted a new test that recognizes privacy rights based on an expectation of privacy. This pivotal change provided a foundation for extending Fourth Amendment protections to include non-trespassory invasions by technologies, such as AI, that do not involve physical entry but could still infringe on privacy.

1 *Katz v. United States*

A seminal case to set the scene of Fourth Amendment protections is *Katz v. United States*, which the US Supreme Court decided in 1967.⁵⁴ *Katz* established the 'reasonable expectation of privacy' test, which comes from Harlan's concurrence. The test is two-pronged and states that (1) an individual must show an actual and subjective expectation to privacy and the expectation is reasonable as well as (2) the expectation must be one that society is prepared to recognize as reasonable.⁵⁵ Harlan further agreed with the majority of the Court that concluded that electronic intrusion into a place that is considered 'private' may certainly constitute a violation of the Fourth Amendment as much as any physical intrusion.⁵⁶ This case created the critical groundwork for determining when technological intrusion by the government violates an individual's reasonable expectation of privacy.

51 U.S. Const. Amend. IV.

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

53 *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967).

54 *Ibid.*

55 *Katz v. United States*, 389 U.S. 347, 361, 88 S. Ct. 507, 516 (1967) (Harlan J., concurring).

56 *Katz v. United States*, 389 U.S. 347, 361-62, 88 S. Ct. 507, 517 (1967).

2 United States v. Jones

Despite the foundation laid by *Katz*, many legal professionals dislike the *Katz* test, considering it to diverge from the original purposes of the Fourth Amendment and have no actual application in today's legal landscape.⁵⁷ Instead, some argue that the *Jones* test is the proper test to follow when considering Fourth Amendment issues, as the test places a greater focus on physical intrusion rather than individual expectations.⁵⁸ In *United States v. Jones*, decided in 2012, some 45 years after the decision brought down by *Katz*, the Court grappled with emerging technologies used in policing.⁵⁹ Here, the Court had to determine whether, under the Fourth Amendment, it is a search or seizure when a global positioning system (GPS) tracking device is attached to a person's car and then used to follow the vehicle's travels on public roads.⁶⁰ Here, the Court stated that the *Katz* holding is an addition to, and does not substitute for, the common law trespass test for which *Jones* doubles down.⁶¹

The Court in *Jones* ultimately determined that the government's installation of the GPS onto the bottom of Jones' car tracked his and subsequently tracked his movements over 28 days was a violation of the Fourth Amendment.⁶² The Court rejected the government's contention that, under the *Katz* test, Jones has no reasonable expectation of privacy in the location of his keep on the public roads and, therefore, the Fourth Amendment had not been violated.⁶³ The issue here does not fall under *Katz*'s purview, the Court says, as there is another, more obvious fact to contend with: the physical intrusion onto Jones' property, that is, his vehicle.⁶⁴ Although not adopted by the majority, the concurrence did consider the implications of a long-term monitoring of an individual's movements utilizing a GPS.

The concurrence, authored by Justice Sotomayor, further grapples with the issue that new modes of surveillance that do not depend upon a physical invasion of property will affect not only the trespassory test here in *Jones* but also how the *Katz* "reasonable expectation of privacy" test will evolve.⁶⁵

II Fourth Amendment Cases and Laws Related to Specific Types of Surveillance

1 Aerial Surveillance

Aerial surveillance is arguably one of the more addressed areas of law enforcement surveillance. However, as surveillance mediums such as drones become increasingly

57 Sophia Z. Lee, 'The Reconciliation Roots of Fourth Amendment Privacy', *The University of Chicago Law Review*, Vol. 91, 2024, p. 2139, 2142-2143.

58 Corrie Thearle, *Jones: A Victory for Fourth Amendment Jurisprudence*, *Jurist* (7 February 2012, 4:00 p.m.), <https://www.jurist.org/commentary/2012/02/corrie-thearle-jones/>.

59 *United States v. Jones*, *supra* note 52.

60 *Ibid.*, at 400, 402.

61 *Ibid.*, at 400, 409.

62 *Ibid.*, at 400, 403.

63 *Ibid.*, at 400, 406.

64 *Ibid.*

65 *Ibid.*, at 400, 415 (J. Sotomayor, concurring).

sophisticated, their integration into police work raises complex legal questions about privacy and the scope of surveillance powers. The existing Supreme Court decisions may not be as applicable or helpful as they once were, given the rapid advancements in drone technology but currently serve as a necessary foundation for approaching drone surveillance-related issues.

(a) *California v. Ciraolo*

In *California v. Ciraolo*, a case from the 1980s, the Court considered the issue of aerial searches within the context of foundational Fourth Amendment practices, namely, *Katz*.⁶⁶ The rule from *Ciraolo* is generally that law enforcement may observe from a publicly accessible viewpoint where they are legally entitled to be.

In *Ciraolo*, Santa Clara Police received an anonymous tip that marijuana was being grown in Ciraolo's backyard.⁶⁷ Since the police could not observe his backyard from the ground due to high fences, they chartered a private plane and flew over the home within navigable airspace. From that vantage point in the air, the police were able to identify marijuana plants growing within Ciraolo's yard and photographed the area.⁶⁸ Applying the *Katz* test, the Court first reasoned that Ciraolo had clearly demonstrated a subjective expectation of privacy given the existence of the two high fences, but they were less inclined to find this expectation as one that society was ready to accept.⁶⁹ The fact that the location is inside the perimeter does not automatically preclude police surveillance, the Court held. There has never been a requirement for law enforcement personnel to cover their eyes when they pass a residence on a public street under the Fourth Amendment's protection of the home clause. Furthermore, an officer has the right to observe from a public vantage point where the activities are clearly visible, and the simple fact that a person has taken steps to limit some views of his activities does not bar law enforcement, or individuals, from doing so.⁷⁰

(b) *Florida v. Riley*

Three years after *California v. Ciraolo*, the Supreme Court once again addressed aerial surveillance when police utilized a helicopter at 400 feet to conduct aerial surveillance.⁷¹ In *Florida v. Riley*, Riley was believed to be growing marijuana in a greenhouse on his property. An officer utilized a helicopter at 400 feet to observe above Riley's property, including the greenhouse, and due to a tenth of the corrugated roofing panels on the greenhouse being inadvertently missing, officers were able to see marijuana growing inside.⁷² Once again the Court applied the *Katz* test,

66 *California v. Ciraolo*, 476 U.S. 207 (1986).

67 *Ibid.*, at 209.

68 *Ibid.*

69 *Ibid.*, at 210-211.

70 *Ibid.*, at 216-217.

71 *Florida v. Riley*, 488 U.S. 445 (1989).

72 *Ibid.*

finding that, while Riley exhibited a subjective expectation of privacy through his enclosed greenhouse, which was obscured from view on the ground level, this would not be sufficient to find that society may recognize this as reasonable. After all, anyone (with a helicopter and plane) can fly at 400 feet above individuals' homes and see the same thing law enforcement can. Therefore, an aerial observation of a constitutionally protected area, such as the home or the curtilage in this case, from a helicopter at an altitude of 400 feet is not a search requiring a warrant under the terms of the Fourth Amendment.

A joint rule developed from *California v. Ciraolo* and *Florida v. Riley* explains that an aerial search is not a search if it (1) is in publicly navigable airspace, (2) is conducted in a physically non-intrusive manner, (3) does not reveal intimate activities and (4) is non-sense enhancing. This test only offers that if these four factors are met, there is not a search under the Fourth Amendment. It does not clarify what if only two or three factors are met or what exactly constitutes a search when aerial surveillance is used. However, it is still instructive as to what influences the Court to find aerial surveillance a search.

Both cases emphasized that if officers are in publicly navigable airspace, whether by helicopter or plane, they are not invading privacy any more than an average citizen would, given that they have the same ability. The intrusive factor recognizes situations like *Jones*, where physical installation or trespass would still constitute a search under the Fourth Amendment. For example, if someone were to utilize a drone to fly into a home, this would be physical trespass and intrusive, making it likely a Fourth Amendment search. Further, if aerial surveillance were to reveal intimate activities, this could make it weigh more towards being a search. After all, one of the factors in the test utilized to term whether an area is curtilage – which is typically constitutionally protected – looks to the way an area is used.⁷³ If an area is used for intimate activities, it may lean more towards being an extension of the home and deserving of Fourth Amendment protections. And, finally, the emphasis on non-sense enhancing gets to the issue of emerging technologies in aerial surveillance and how those may weigh towards the surveillance being a search. This will be discussed further in the subsection directly on non-sense-enhancing caselaw.

2 Sense-Enhancing Technology

(a) *Kyllo v. United States*

One crucial test that examines the conjunction of the Fourth Amendment and emerging technologies is derived from *Kyllo v. United States*.⁷⁴ In *Kyllo*, the Court had to grapple with the use of a thermal-imaging device aimed at a private home that was being used to detect heat using through-the-wall technology.⁷⁵ Here, the State attempted to argue that the thermal imaging was constitutional because it merely detected heat radiating from the outside of the home, the device provided only the basis of inferences

⁷³ *United States v. Dunn*, 480 U.S. 294 (1987).

⁷⁴ *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038 (2001).

⁷⁵ *Ibid.*

and it did not “detect private activities occurring in private areas”.⁷⁶ However, the Court rejected this argument stating that the State’s arguments do not follow the logic of *Katz*, where the Court had determined that sound waves emanating from a phone booth were protected under the Fourth Amendment.⁷⁷ Further, the Court determined that, within the home, all details are considered intimate.⁷⁸

The test for *Kyllo* is as follows: there has been a search when, by sense-enhancing technology, any information regarding the interior of the home that otherwise could not have been obtained without physical intrusion into a constitutionally protected area, at least where, as in *Kyllo*, the technology in question is not in general public use.⁷⁹ There is no substantive case law on what ‘general public use’ means in this context. Therefore, the *Kyllo* test is very narrow and applies only to certain types of technology.

3 Cellphones and Their Data

(a) *Riley v. California*

The Court held that the police may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.⁸⁰ While the State argued that the search of a cell phone post-arrest is equivalent to a search of physical items, the Court disagreed because of the implicit privacy concerns associated with the cumulation of data cell phones have stored.⁸¹ An exception to the warrant requirement is normally determined

by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.⁸²

In *Riley*, the Court deemed the intrusion on such a large scale into cell phone data on an individual outweighed that of any governmental interests. Therefore, the Court affirmed that searches of large quantities of data require a warrant under the Fourth Amendment (Figure 1).⁸³

⁷⁶ *Kyllo* at 533 U.S., at 29, 121 S. Ct., at 2040.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

⁷⁹ *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038 (2001) (rule derived from entirety of the case).

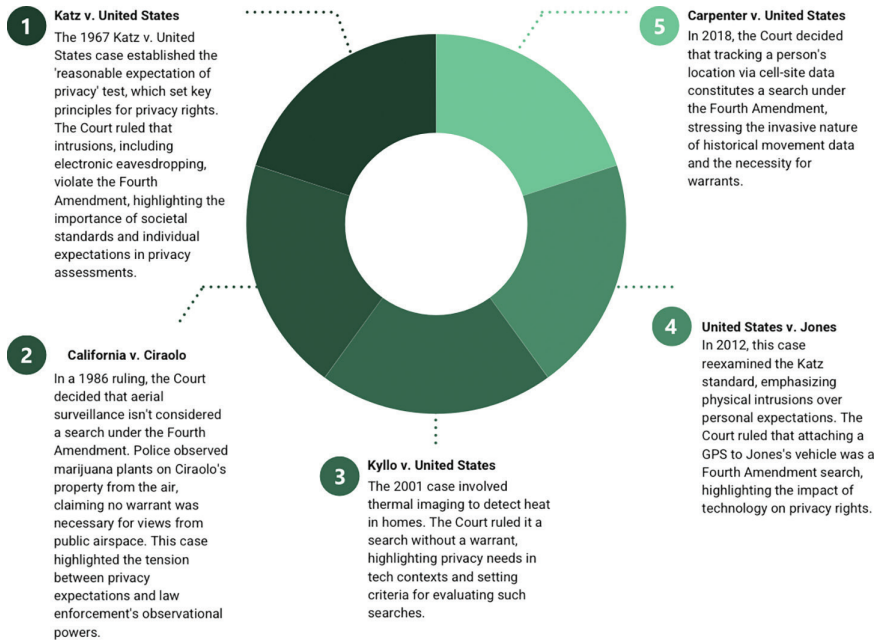
⁸⁰ *Riley v. California*, 573 U.S. 373, 403 (2014).

⁸¹ *Ibid.*, at 373, 393.

⁸² *Ibid.*, at 373, 385.

⁸³ *Riley v. California*, *supra* note 81.

Figure 1 *Generated by Vengage, an AI platform.*



4 *The Internet and AI* (ACLU v. Clearview AI)

ACLU v. Clearview AI is a lawsuit originating from 2020 where the ACLU and ACLU of Illinois sued Clearview AI for violating the Illinois Biometric Information Privacy Act (BIPA).⁸⁴ Clearview AI, an American facial recognition company, provides software primarily to law enforcement and government agencies with the function of matching faces to a database of more than 50 billion images collected from the internet.⁸⁵ The collection of these images is called a 'faceprint', a biometric identifier that may be used to verify a person's identity.⁸⁶ Clearview creates these faceprints by scanning a photo, measuring and recording the data of facial characteristics such as the distance between features and then assigning the data a numerical value.⁸⁷ The data is collected into their database, categorizing similar faceprints together.⁸⁸ Clearview then sells access to its technology, database and investigative tools to both public and private entities, without permission by individuals to create or store faceprints.⁸⁹

Although the lawsuit brought by the ACLU focused mainly on harm this technology may cause on domestic violence and sexual assault survivors, undocumented

⁸⁴ *ACLU v. Clearview AI*, ACLU (May 11, 2022), <https://www.aclu.org/cases/aclu-v-clearview-ai>.

⁸⁵ Clearview AI, <https://www.clearview.ai>.

⁸⁶ *ACLU v. Clearview AI, Inc.*, 2021 Ill. Cir. LEXIS 292, at *1.

⁸⁷ *Ibid.*

⁸⁸ *Ibid.*

⁸⁹ *Ibid.*, at *1-2.

immigrants and members of vulnerable communities, the Cook County Circuit Court also considered the concerns in the context of significant public interest to all.⁹⁰

The ACLU's lawsuit against Clearview AI demonstrates the need for comprehensive AI regulation to ensure that biometric data is collected ethically and used in a reasonable manner. BIPA serves as a model for such regulation, emphasizing the necessity of obtaining explicit consent from internet users before collecting biometric information. The aggregation of faceprints by Clearview AI creates a detailed and invasive picture of individuals' lives. According to the Mosaic Theory, this extensive data collection should be considered a search, thus requiring adherence to Fourth Amendment standards to protect citizens' privacy. The case also highlights broader ethical concerns about the use of AI in surveillance, and by ensuring transparency, accountability and respect for privacy rights, we can work to maintain public trust and protect vulnerable communities from potential harm.

5 *The Mosaic Theory: How Individual Data Points Can Create a Comprehensive Picture*

Traditional Fourth Amendment analyses by the courts have evaluated each investigative step individually to determine if a search has occurred. However, with the emergence of advanced surveillance technologies this approach has been reevaluated, and thus, the Mosaic Theory was born. As Paul Rosenzweig, an attorney and expert in national security and privacy law, put simply:

the 'mosaic theory' is the idea that large scale or long-term collections of data reveal details about individuals in ways that are qualitatively different than single instances of observation and the related idea that as a consequence Fourth Amendment law should take account of that fact through a warrant requirement for 'big data' collection.⁹¹

Clear as mud? Contextualization may help to clarify the theory and its reasoning.

The Mosaic Theory came to fruition in the case *United States v. Maynard*, where the DC Circuit reasoned that searches may be analysed as a collective sequence rather than individual steps and requiring the police to analyse a collective 'mosaic' of surveillance would provide a more comprehensive analysis of a search under the Fourth Amendment.⁹² According to the court in *Maynard*, GPS tracking of a vehicle's whereabouts for 28 days amounts to so much monitoring that the entire sequence qualifies for Fourth Amendment protection.⁹³ This opinion prevailed in concurring opinions in *Jones* written by Justice Alito and Justice Sotomayor as they utilized the reasoning in *Maynard* in support of the Mosaic Theory.⁹⁴

90 *ACLU v. Clearview AI*, ACLU (Last updated 11 May 2022), <https://www.aclu.org/cases/aclu-v-clearview-ai>.

91 Paul Rosenzweig, *In Defense of the Mosaic Theory*, lawfare (29 November 2017, 3:18 p.m.), <https://www.lawfaremedia.org/article/defense-mosaic-theory#postContributors>.

92 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 314 (2012).

93 *United States v. Maynard*, 392 U.S. App. D.C. 291 (2010).

94 Kerr, *supra* note 92.

In Alito's concurrence, for which Justices Ginsburg, Breyer and Kagan joined, he stated as follows:

Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society'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.⁹⁵

Here, Alito argues that short-term surveillance of a person's movements in a public setting does not violate traditional societal expectations of privacy. Short-term public monitoring is almost to be expected by individuals in society and, therefore, that expectation is reasonable. The invasiveness of long-term monitoring overcomes this reasonable expectation of privacy as this type of monitoring reveals detailed patterns of an individual's life. Alito's reasoning is rooted in the same logic as the Mosaic Theory, suggesting that the aggregation of data over time creates a comprehensive picture of an individual's life and that this cumulative effect constitutes a search under the Fourth Amendment. In *Jones*, the extensive four-week tracking clearly crossed the line into a search, triggering Fourth Amendment protections.⁹⁶

(a) *Carpenter v. United States*

The adoption of the Mosaic Theory by courts has been a contentious topic, with many experts arguing that the theory presents problems for analysing Fourth Amendment cases instead of evolving with the ever-changing landscape of modern technology. This is even more true post-*Carpenter*, where the Supreme Court held that historical cell-site location information (CSLI) would allow the government “near perfect surveillance” of cell phone users' physical location when used for a period longer than seven days.⁹⁷ Chief Justice Roberts, writing for the majority, emphasized that CSLI provides an “intimate window into a person's life”, revealing not just their location, but their associations and activities as well.⁹⁸ This extensive tracking, therefore, violated reasonable expectations of privacy.

Scholars argue that the classic technique of figuring out when government conduct qualifies as a search amendment protection, known as the ‘sequential

95 *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J, concurring) (citation omitted).

96 *Ibid.*, at 400, 430-431 (2012) (Alito, J, concurring).

97 *Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206 (2018); see also Robert Fairbanks, ‘Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-*Carpenter*’, *Berkeley Journal of Criminal Law*, Vol. 26, 2021, p. 71.

98 *Carpenter v. United States*, 585 U.S. 296, 311, 138 S. Ct. 2206, 2217 (2018).

approach', is in opposition to the Mosaic hypothesis. Consequently, a particular investigation method may be regarded as a search in one instance, but it may not be in another because the combined data provided less information.⁹⁹

For the purposes of this article, the Mosaic Theory is analysed in conjunction with the Fourth Amendment and emerging AI technology regardless of its potential pitfalls or critiques. As the US Supreme Court has yet to renounce this approach, the Mosaic Theory is still an influential piece of doctrine that will certainly be considered by both the Supreme Court and lower courts as AI technology continues to move into governmental tactics of security and presents privacy and freedom concerns for US citizens.

C Challenges Presented by AI Technologies in Law Enforcement

As described in Part I, AI such as facial recognition and BWCs have significantly expanded the capabilities of law enforcement and raise critical questions about privacy and accountability.¹⁰⁰ Case law has demonstrated that the scope and scale of data collection are determined by what constitutes a search under the Fourth Amendment, and these analyses may be inconsistent depending on whether the court is applying the Mosaic Theory or the traditional step-by-step process.¹⁰¹

Another challenge posed is derived from what is called the 'Third-Party Doctrine', a legal principle that states that individuals have no reasonable expectation of privacy for information voluntarily shared with third parties, such as phone companies or internet service providers.¹⁰² AI surveillance often relies on data from these third parties and also shares its own data with third parties, challenging the applicability of this doctrine.¹⁰³ Would this exchange of information between third parties, if requested by the government, count as continuous and pervasive monitoring subject to analysis under the Mosaic Theory? Given what we know of *Carpenter*, the idea does not seem so far-fetched.

Transparency and accountability are also challenges due to the complex nature of AI systems. The application of technological methodologies, tools and techniques to make AI systems intelligible, interpretable and auditable is the main focus of technical approaches to transparency and accountability in AI systems. These methods seek to shed light on how AI systems make decisions, spot possible biases or mistakes and empower people to understand and question the results of these systems.¹⁰⁴ Deep learning neural networks used in algorithms for AI are frequently 'black boxes' with internal workings that are impossible for humans to understand.¹⁰⁵

99 Fairbanks, *supra* note 97.

100 See *supra* Part I.

101 See *supra* Part II.

102 See *United States v. Miller*, 425 U.S. 435 (1976).

103 Katharine Miller, *Privacy in an AI Era: How Do We Protect Our Personal Information?*, Stanford University: Human-Centered Artificial Intelligence (18 March 2024), <https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>.

104 Ben Chester Cheong, 'Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making', *Frontiers in Human Dynamics*, Vol. 6, No. 1, 2024, p. 2.

105 *Ibid.*

In instances where AI is used in high-stakes decision-making contexts, such as by law enforcement officials when making an arrest or conducting an investigation, strong social interests exist in being able to comprehend how the system functions, challenge its results and demand explanations for actions influenced by these algorithms.¹⁰⁶ The EU AI Act is one such regulatory framework looking towards mandated transparency for high-risk AI systems.¹⁰⁷ Transparency and accountability are needed not only in broad areas of AI regulation but also specifically with AI technologies used by law enforcement.

I Impact of AI Surveillance on Privacy and Civil Liberties: A Case Study

This section delves into a case study that highlights the multifaceted impact of AI surveillance. In understanding AI surveillance utilized by law enforcement, it is crucial to consider real-world examples to contextualize the issue within the modern world. Through this case study, this article will explore how AI surveillance can both protect and infringe upon Fourth Amendment rights, emphasizing the need for thoughtful and balanced regulation.

1 San Francisco's Ban on Facial Recognition Technology

In 2019, San Francisco became the first major city in the US to ban local government agencies' utilization of facial recognition. The ordinance dubbed 'Stop Secret Surveillance' passed 8-1 in a vote by the city's board of supervisors and constitutes a full ban on facial surveillance in multiple government agencies, including police departments and prisons.¹⁰⁸ These facial recognition technologies have the ability to detect faces in images or videos and match characteristics to identities within different databases.¹⁰⁹ New facial recognition technologies are more precise than traditional facial detection used by law enforcement, and AI will only continue to improve the technology.¹¹⁰

Along with the ban on facial recognition technology, San Francisco is also requiring city agencies to get city approval before acquiring various types of surveillance technologies, including automatic licence plate readers and camera-equipped drones.¹¹¹ San Francisco city officials seem to be concerned about the chilling effects this technology has on civil rights and civil liberties, such as racial injustice and continuous observation from the government.¹¹²

The San Francisco Police Department (SFPD) will be the most affected by this ordinance as they will not be able to test any facial recognition tools in criminal investigations. While the SFPD has not outwardly opposed or denied the use of facial recognition technology in their investigations, the department has called for balancing

106 *Ibid.*, at 3.

107 *Ibid.*

108 Shirin Ghaffary, *San Francisco's Facial Recognition Technology Ban, Explained*, VOX (14 May 2019, 7:06 p.m.), <https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained>.

109 *Ibid.*

110 *Facial Recognition & Law Enforcement – The Value Proposition*, AWARE (16 February 2023), <https://www.aware.com/blog-facial-recognition-used-in-law-enforcement/>.

111 Ghaffary, *supra* note 108.

112 *Ibid.*

both the privacy concerns and the potential public safety benefits that come with utilizing these technologies.¹¹³ The ban will not, however, restrict surveillance technology utilized in the San Francisco International Airport as the Transportation Security Administration and Customs and Border Patrol have jurisdiction.¹¹⁴ This also makes sense in the Fourth Amendment context as Fourth Amendment protections have traditionally been left at baggage check along with one's luggage.

Despite this groundbreaking ordinance, in the five years since its implementation, the SFPD has now admitted to evading the restriction six times.¹¹⁵ However, previously undisclosed documents indicate that the issue is more serious than the SFPD acknowledges and that there might be justification for reviewing and dismissing dozens or even hundreds of criminal cases. There may be at least seven more violations as officers admit to requesting that nearby agencies use the technology for them, according to documents referenced in a complaint filed in the summer of 2024 against the city by Secure Justice, a non-profit organization that works to prevent government overreach.¹¹⁶

The unauthorized use of facial recognition technology by the SFPD could be seen as a violation of the Fourth Amendment, which protects against unreasonable searches and seizures. The Fourth Amendment requires that searches and seizures be reasonable, often necessitating a warrant. The use of facial recognition technology without proper authorization or oversight could be considered an unreasonable search, especially given the potential for mass surveillance and the collection of biometric data without consent. Further, depending on how pervasive the continued use of facial recognition technology was in the instant case, the cumulative use of the facial technology by the SFPD may collectively create a comprehensive surveillance system under the Mosaic Theory and violate the public's reasonable expectation of privacy.

The SFPD's violations demonstrate what the city's government was looking to avoid in the first place by implementing the ordinance: use of facial recognition technology, especially when combined with other surveillance tools like automatic licence plate readers and camera-equipped drones, to create a detailed profile of individuals. This aggregated data can reveal patterns of behaviour, associations and movements, which constitutes a search under the Fourth Amendment.¹¹⁷ Further, the violations here underscore the necessity for oversight and accountability when utilizing these sorts of technologies. Without proper checks by regulating authorities, the aggregation of surveillance data can lead to significant Fourth Amendment violations. Judicial oversight here may help ensure that surveillance practices are transparent and respect individuals' privacy rights.

113 *Ibid.*

114 *Ibid.*

115 Jennifer Wadsworth, *SFPD Skirted Facial-Recognition Ban, Lawsuit Says. Hundreds of Cases Could Be in Jeopardy*, The San Francisco Standard (18 July 2024, 8:00 a.m.), <https://sfstandard.com/2024/07/18/san-francisco-police-facial-recognition-violations/>.

116 *Ibid.*

117 See *Carpenter v. United States*, 138 S. Ct. 2206 (2018); see also *United States v. Maynard*, 392 U.S. App. D.C. 291 (2010).

D Current Legal Frameworks

A number of current legal frameworks may be used to help guide future regulations and laws regarding AI surveillance and law enforcement use. These existing frameworks include the Guiding Principles on Government Use of Surveillance Technologies, the Stored Communications Act (SCA) and Executive Order 14110. By analysing these legal frameworks to see how AI is already being regulated, we can address existing gaps in regulation.

I *Guiding Principles on Government Use of Surveillance Technologies*

In line with their international commitments and duties, governments can maintain their commitment to uphold and defend democratic values, human rights and fundamental freedoms through the responsible use of surveillance technology by adhering to these voluntary and non-binding ‘Guiding Principles’ created by the Freedom Online Coalition (FOC). In three key areas of concern, these Guiding Principles aim to stop governments and individuals working on their behalf from abusing surveillance technologies.¹¹⁸ One specific area of concern for these Guiding Principles is “[p]airing advanced video surveillance with artificial intelligence (AI)-driven [*sic*] tools to persistently identify and monitor people without an appropriate legal basis”.¹¹⁹

The Guiding Principles include many guidelines governments should follow. One such principle looks to limit the amount and type of data gathered using surveillance technology, as well as the duration for which that data is kept, which should be restricted to that which is pertinent, required and appropriate to accomplish specific and lawful goals of public interest.¹²⁰ Biometric tools like fingerprint scans, DNA analytics, facial recognition, speech recognition, gait recognition and iris scans should only be used in this context when it is legal and appropriate, taking into account the context of collection and use and weighing the interests involved.¹²¹

Another such principle includes keeping AI surveillance use in conformance with the Fourth Amendment. Mechanisms that prevent and address violations of relevant domestic law should be put in place by governments, such as in the context of potential Fourth Amendment violations when it comes to searches utilizing AI.¹²² Clear definitions, regular practise, equitable enforcement and reviews for unforeseen effects or misuse are all necessary for efficient supervision, transparency and redress procedures.¹²³ Access to suitable and efficient judicial or extrajudicial remedies should be available to everyone seeking such remedy, this principle states.¹²⁴

118 *Guiding Principles on Government Use of Surveillance Technologies*, Freedom Online Coalition (March 2023), <https://www.state.gov/wp-content/uploads/2023/03/FOC-FINAL-Surveillance-Principles-03092023.pdf>.

119 *Ibid.*

120 *Ibid.*

121 *Ibid.*

122 *Ibid.*

123 *Ibid.*

124 *Ibid.*

II The SCA

The SCA is part of the Electronic Communications Privacy Act, providing protections for stored electronic communications held by service providers.¹²⁵ The SCA's legal framework is rooted in the Fourth Amendment and was passed by Congress to address growing concerns regarding the Third-Party Doctrine, emerging technologies and government oversight.¹²⁶ Relevant sections of the SCA include Section 2701, the SCA's broad ban on purposefully accessing stored electronic communications without permission in order to obtain, modify or block access to those communications; Section 2702, which forbids companies that offer the public remote computing services (also known as RCS, like cloud computing providers) and electronic communication services (also known as ECS, like cell phone, email or social media platforms) from wilfully disclosing communications stored in electronic storage to any individual or organization; and Section 2703, which describes how government agencies can use an administrative subpoena, a court order or a warrant to force providers to reveal information about electronic communications.¹²⁷ Of course, all of these sections provide exceptions for certain governmental interests, as most legal frameworks do.

In terms of AI regulation, the SCA governs how this data can be accessed and used by law enforcement and government entities, ensuring that privacy protections are in place. Governments must comply with the SCA's warrant requirement, which is rooted in the Fourth Amendment. SCA provides a legal framework that AI systems utilizing public data must follow to ensure the protection of privacy of individuals. The SCA will certainly need to evolve with emerging AI technologies and ensuring that governmental use of AI surveillance technologies that use big data sets from third parties and comply with legal frameworks such as the SCA will be crucial for maintaining public trust.

However, these traditional legal frameworks and guidelines may prove difficult to enforce with AI-driven surveillance technology given the *sui generis* nature of the problems that are created by this new technology. How will current legal frameworks be adapted to better regulate AI surveillance technology, especially when it comes to government compliance?

III Executive Order 14110

In 2023, President Biden issued Executive Order 14110, which focuses on the safe, secure and trustworthy development and use of AI, including in the law enforcement arena. This executive order contemplates different ways law enforcement uses or may use AI with existing enforcement and investigatory tools, including automated licence plate readers, security cameras embedded with facial recognition and BWCs, which may use AI software to redact or blur faces or sensitive footage.¹²⁸

125 Jimmy Balser, Cong. Rsch. Serv., LSB10801, Overview of Governmental Action Under the Stored Communications Act (SCA) 1 (2022), <https://crsreports.congress.gov/product/pdf/LSB/LSB10801>.

126 *Ibid.*, at 1-2.

127 *Ibid.*

128 Kristin Finklea, Cong. Rsch. Serv., IN12289, Law Enforcement Use of Artificial Intelligence and Directives in the 2023 Executive Order 1-2 (2023), <https://crsreports.congress.gov/product/pdf/IN/IN12289>.

The executive order considered many concerns regarding AI use in law enforcement, including whether it reinforces preconceptions. One argument is that biased data is used to train the software, which in turn feeds prejudice into the AI systems.¹²⁹ Another worry is that authorities may disregard conflicting evidence as a result of their dependence on AI technology. To assess and mitigate some of the issues, policymakers might think about stepping up oversight of police usage of AI systems.¹³⁰

Executive Order 14110 includes multiple directives concerning how to ensure accountability in federal law enforcement with regard to the utilization of AI in surveillance and investigative technologies. These directives include the Attorney General's (AG) coordination and enforcement of federal laws to address any discrimination or civil rights violations perpetuated by the use of AI-enhanced technologies.¹³¹ By addressing these concerns, the hope is to address algorithmic discrimination from the jump and prevent further discriminatory practices. Another directive focuses on protecting privacy rights and other civil liberties. This directive details that the AG, with the Homeland Security Secretary and the Office of Science and Technology Policy Director, will submit reports to the President on the use of AI in the criminal justice system.¹³² Further, an interagency working group that was established by Executive Order 14074 will work with law enforcement agencies to implement practices for recreating and training officers with AI expertise.¹³³ These practices may be recommended to state, local, tribal and territorial law enforcement agencies as well.¹³⁴

IV Gaps in the Current Legal Framework

According to experts, including Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights while countering terrorism, "Urgent and strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition".¹³⁵ The experts emphasized the need to make sure that these systems do not expose individuals and communities to more human rights abuses, such as the growth and misuse of intrusive surveillance methods that violate privacy rights and domestic law.¹³⁶ Some gaps in regulation, the United Nations (UN) states, include more transparency in large-scale data collection and strong end-to-end encryption to secure digital communications.¹³⁷

Currently, there is no overarching federal law that specifically focuses on regulating the use of AI in law enforcement. Foundational case law, such as *Katz*, *Jones* and *Maynard*, was not created with the idea of AI technologies in mind. With this, the application of these rules to Fourth Amendment challenges regarding AI

129 *Ibid.*, at 2.

130 *Ibid.*

131 *Ibid.*

132 *Ibid.*

133 *Ibid.*

134 *Ibid.*

135 *Regulation Essential to Curb AI for Surveillance, Disinformation: Rights Experts*, United Nations (2 June 2023), <https://news.un.org/en/story/2023/06/1137302>.

136 *Ibid.*

137 *Ibid.*

surveillance by law enforcement and government entities is ambiguous at best. Even the Mosaic Theory, a more recent doctrine that considers the aggregation of large data pools, such as those used by AI, is not precisely on point. This raises the question, should judges, regulatory bodies and decision-makers utilize already established frameworks to consider these issues? Or, should the US be working to develop AI-specific rules and regulations regarding Fourth Amendment and privacy concerns?

E Recommendations and Solutions

I Utilizing Existing Resources

The protections offered by the Fourth Amendment are largely interpreted through case law rather than explicit statutes, which informs the context of our recommendations. Notably, 42 US Code § 1983 already provides a mechanism for civil action in cases of rights deprivation, including those pertaining to Fourth Amendment violations.¹³⁸ This existing statute is a potent tool for individuals to challenge and seek redress for infringements arising from the use of AI in law enforcement. A potential recommendation related to the use of § 1983 claims is to require the publishing of data related to § 1983 claims specifically related to AI-enhanced law enforcement surveillance. This would require outlining detailed reporting requirements as to what is considered AI-enhanced law enforcement surveillance and what is not. Over time, this data would provide insights into whether there is an increasing trend in claims related to AI surveillance, helping to assess whether this issue is escalating in significance.

The fundamental challenge in regulating AI use within law enforcement is the absence of comprehensive guidelines for managing AI technologies overall, including those underpinning emerging tools. For instance, generative AI, which can fabricate highly realistic but false images and videos, currently operates without substantial federal oversight. An effective approach to address these regulatory gaps would involve establishing universal regulations for AI applications.

However, there could be statutes created to regulate the use of AI surveillance in law enforcement directly to set guidelines, as discussed below.

II Transparency and Accountability

Another recommendation is mandating transparency in AI surveillance practices. This can be accomplished by requiring agencies to disclose the AI tools used and their impact, as well as creating guidelines on types of AI and the limits to which police can use AI in their investigations. As demonstrated with Project Maven, the public is weary of AI use in projects in which the goals, usage and potential risks are not communicated to the public.¹³⁹

We have seen some governmental entities creating comprehensive outlines for the ethical use of AI in surveillance.¹⁴⁰ The current Guiding Principles put forth by

¹³⁸ 42 U.S.C. § 1983 (2024).

¹³⁹ See *supra* Part ____.

¹⁴⁰ See *supra* Part ____.

the FOC can be expanded on. The lawfulness principle should be extended so that surveillance activities by law enforcement departments must be authorized by law. Through this, citizens will have public access to the rules that regulate AI surveillance utilization by law enforcement agencies, and they can be made aware of the circumstances under which their data may be collected and used. This law should include provisions that state that surveillance should only be conducted when necessary for achieving a legitimate aim, such as national security or public safety, for which other reasonable means would be insufficient. The measures taken must be proportionate to the aim of the surveillance, ensuring minimal intrusion into individual's privacy and ensuring their reasonable expectations are maintained under *Katz*. Reasonableness is the cornerstone here as AI surveillance use by law enforcement should not be unjust or arbitrary, and each utilization must consider the impact on an individual's rights and protections under the Fourth Amendment.

Government agencies should also implement robust mechanisms to prevent violations of the Fourth Amendment. By conducting regular Fourth Amendment impact assessments before deploying surveillance technologies, constitutional rights can be safeguarded before violations occur. This may include data protection given that many AI databases utilize vast amounts of personal information mined by third parties.¹⁴¹ This is important not only for individual privacy rights but also to ensure that investigations and evidence collected from these investigations are not thrown out under the exclusionary rule due to an unreasonable search or seizure.

There are many existing frameworks that govern other aspects of law that may be helpful in updating existing Guiding Principles or creating new ones. Existing frameworks include the European Convention on Human Rights (ECHR) Article 8, which protects the right to privacy and sets out conditions under which surveillance may be justified.¹⁴² Specifically, ECHR Art. 8 begins with the following simple phrase: "Everyone has the right to respect for his private and family life, his home and his correspondence".¹⁴³ This ideal is similar to that put forth by the Fourth Amendment, preventing unreasonable governmental intrusion on individual privacy rights. Art. 8 puts forth instances in which public authority may interfere with this right, such as in accordance with the law and in doing what is necessary in the interests of a democratic society.¹⁴⁴ Thus, this framework is a good springboard for the US to begin to create its own guideposts regarding AI surveillance.

III Warrant Requirement and Probable Cause

One of the biggest challenges that comes with resolving constitutional concerns surrounding AI surveillance in law enforcement investigations is the warrant and probable cause requirements of the Fourth Amendment. With no existing case law directly on point, strengthening the warrant requirements for AI surveillance is a

¹⁴¹ See Miller, *supra* note 103.

¹⁴² European Convention on Human Rights, Art. 8, 4 November 1950, 213 U.N.T.S. 221.

¹⁴³ *Ibid.*

¹⁴⁴ *Ibid.*

large gap in current legal frameworks. Addressing this gap is crucial for protecting the sanctity of the Fourth Amendment.

While there have been recent executive orders put forth by President Biden, such as Executive Order 14110, and a number of state regulatory actions,¹⁴⁵ none of these have addressed AI surveillance in the context of the Fourth Amendment. One way to bridge this gap is by enacting specific laws or developing case laws that govern the use of AI in surveillance, ensuring that they align with Fourth Amendment protections. These laws or judicial rulings should define the circumstances under which AI surveillance can be used and require warrants based on probable cause or intrusive surveillance methods. These rules should take into consideration existing case law, such as the reasonable expectation of privacy in *Katz* and the aggregation of large quantities of data in the Mosaic Theory.

Utilizing the foundational ruling in *Katz*, new laws should explicitly state that AI surveillance technologies must respect an individual's reasonable expectations of privacy. As this expectation is ever-changing due to the rapid development of new technology, a new determination of what 'reasonable expectation' means in the context of AI surveillance is important. Any surveillance that intrudes upon areas where individuals have a reasonable expectation of privacy, such as in the home, the surrounding property or private communications, should require a warrant based on probable cause. By ensuring that there are no ambiguities when it comes to whether AI surveillance should be subject to strict warrant requirements similar to traditional surveillance methods, Fourth Amendment protection will be safeguarded.

The Mosaic Theory should also be implemented into these new laws or rulings. This can be accomplished in the form of data aggregation limits and compressive warrants. News laws should recognize that, under the Mosaic Theory, a prolonged and comprehensive collection of data through AI surveillance can amount to a search. Therefore, even if individual data points are collected lawfully by AI surveillance, their aggregation over an extended period of time, such as seven days,¹⁴⁶ should be subject to Fourth Amendment protections. Comprehensive warrant requirements are also essential. By requiring warrants to include the specific duration and scope of surveillance allowed, overly broad or indefinite monitoring can be prevented. Such monitoring would be akin to a general warrant, the prevention of which is one of the main goals of the Fourth Amendment.¹⁴⁷

IV Oversight and Judicial Review

None of these new regulations, laws or rulings will be of significance without independent oversight bodies to enforce them. One model to consider in developing

145 Sagar K. Ravi, et al., *AI and The Law: Emerging Trends in Enforcement*, MWE (19 December 2024), <https://www.mwe.com/insights/ai-and-the-law-emerging-trends-in-enforcement/>.

146 *Carpenter v. United States*, *supra* note 97.

147 See Generally *Amdt 4.2 Historical Background of the Fourth Amendment*, Constitution Annotated, https://constitution.congress.gov/browse/essay/amdt4-2/ALDE_00013706/ (accessed 20 December 2024).

this oversight body is the Privacy and Civil Liberties Oversight Board.¹⁴⁸ This board was established to ensure that efforts to protect the US from terrorism do not infringe on individual privacy and civil rights. A similar ideology can be followed to ensure that law enforcement's use of AI surveillance does not infringe upon Fourth Amendment protections and other civil liberties.

Having not only legal professionals but also AI experts on this board is essential. AI experts, such as Geoffrey Hinton (also known as one of the 'Godfathers of AI') and Dr. Fei-Fei Li (the former Chief Scientist in AI/Machine Learning at Google Cloud),¹⁴⁹ have the practical and scientific knowledge surrounding AI and machine learning to better inform what regulations can practically be put in place and how to enforce them. While legal and judicial professionals will know the best way to create and interpret these new laws and regulations, expertise on how AI surveillance technology is created and works on a technical level will be crucial in creating practical laws.

The new regulatory body should conduct regular audits of AI surveillance technologies and how they are used. These audits should be made available to the public to keep them informed on the oversight being put into these practices, as well as provide a location for individuals to go to if they wish to learn more about the technology and how it is used. These audits can be published in conjunction with transparency reports that may include the use of AI surveillance technologies, including the number of warrants that have been obtained by law enforcement, the types of data collected and the outcome of AI-assisted investigations. This mandate of public disclosure will help solve some issues of public fear when it comes to AI use in official investigations.

Finally, the Supreme Court should consider deciding a case that specifically puts forth a test for considering when AI surveillance by law enforcement encroaches on Fourth Amendment protections. Their decision should further address whether AI surveillance should meet traditional probable cause standards or some sort of heightened standard, perhaps in the context of the Mosaic Theory. The violation by the SFPD of San Francisco's facial recognition ordinance may be a good case to start with as they can also set forth penalties that law enforcement departments may face when they use AI in contravention of proscribed regulations.

F Conclusion

AI is a hot topic at the moment. According to *Scholastica*, 'artificial intelligence' is one of the twenty-five most-used keywords for articles accepted by it in 2024.¹⁵⁰ With the wide range of challenges and considerations that come with integrating AI into our every day, it is clear to see why this topic is so prevalent. The integration

148 U.S. Privacy and Civil Liberties Oversight Board, <https://www.pclob.gov> (accessed 20 December 2024).

149 Great Learning Editorial Team, *Top 12 AI Leaders and Researchers You Should Know in 2024*, Great Learning (27 September 2024), <https://www.mygreatlearning.com/blog/ai-researchers-and-leaders/>.

150 *What Legal Scholars Are Writing About: 2024 Edition*, Scholastica, <https://blog.scholasticahq.com/post/legal-scholars-writing-about-2024/>.

of AI into law enforcement practices is just one of these profound challenges. As AI technologies such as facial recognition, predictive policing and automated LPR become more prevalent, they offer unprecedented efficiency and accuracy in policing. However, these advancements also raise critical concerns regarding privacy, civil liberties and potential abuse.

The Fourth Amendment protection against unreasonable searches and seizures must evolve with AI due to its unique complexities. Key legal precedents such as *Katz v. United States*, *United States v. Carpenter* and the Mosaic Theory provide a foundational framework for understanding how AI surveillance intersects with constitutional rights. These rulings highlight the importance of maintaining a reasonable expectation of privacy and recognizing the cumulative impact of data aggregation.

In order to bridge the gap between AI surveillance and the Fourth Amendment, analysing existing case studies and legal frameworks, as well as enacting regulatory and legal measures, is essential. These legal measures should include leveraging existing laws like 42 US Code § 1983 for civil action in cases of rights deprivation, mandating transparency practices in AI surveillance, strengthening warrant requirements, recognizing the Mosaic Theory in new laws, establishing independent oversight bodies and involving AI experts in the regulatory process.

This article calls for a balanced legal framework that leverages the benefits AI brings to national security and public safety while safeguarding individual rights. By ensuring transparency, accountability and adherence to Fourth Amendment protections, we can both benefit from these evolving technologies and ensure that our data is not infringing on our constitutional rights.