Journal of Business & Technology Law

Volume 18 | Issue 2 Article 3

# Fourth Amendment Constraints on Automated Surveillance Technology in the Public to Safeguard the Right of an Individual to be "Secure in Their Person"

Srivats Shankar

# Fourth Amendment Constraints on Automated Surveillance Technology in the Public to Safeguard the Right of an Individual to be "Secure in Their Person"

**SRIVATS SHANKAR***


## ABSTRACT

Law enforcement throughout the United States is adopting automated surveillance technology, like facial recognition, at breakneck speeds. The use of such technology is often not approved by a legislative body. Yet, the public is subject to this technology, and incorrectly identified and arrested from misidentification. As automated surveillance technology proliferates, it directly conflicts with constitutional traditions. In particular, the Fourth Amendment protection against search and seizure would limit the use of such technology. Although courts have not addressed the growing specter of automated surveillance technology in depth, its impact will likely result in judicial review, especially its use in the public where privacy expectations have traditionally been lower. The Fourth Amendment requirement for "particularity" places an acute limitation on broad dragnet style automated surveillance systems, which requires that law enforcement particularly identify the place or person to be searched or seized. This article addresses the need to develop jurisprudence that tackles the problem of automated surveillance technology and provides recommendations on how courts can address the use of this technology, as well as suggest remedies that can limit injury caused by the unlawful use of this technology.


## INTRODUCTION

On June 18, 2020, police arrested Robert Julian-Borchak Williams at his home.[1] His wife and daughters were present, distraught with what they were seeing.[2] When Williams' wife asked what he was under arrest for, the officers simply replied,

* © Srivats Shankar, Esq., University of California, Irvine School of Law (JD 2022). I would like to thank Professor David Kaye for his guidance and feedback in preparing this article. I would also like to thank my parents, Ashoka and Shankar, and my brothers, Aditya and Partha, for their ever-continuing support. All thoughts are my own and should not be attributed to anyone else.

1. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

2. *Id.*

"Google it."[3] An hour earlier, he sat in his office, where he got a phone call from the Detroit Police Department.[4] Officers told him to come to the station to be arrested. Williams thought the call was a prank.[5] Following his arrest, Williams was handcuffed, fingerprinted, his DNA was collected, and he was held in jail overnight. The next day, the police took Williams to an interrogation room and showed him a surveillance video of a heavy man dressed in black shoplifting $3800 worth of goods from a boutique store.[6]

The detective asked Williams, "is this you?" "No, this is not me," said Williams. "You think all black men lookalike?"[7]

Williams' case represents one of a series where facial recognition system incorrectly identified a suspect.[8] His story is neither the first, nor will it be the last.

Williams' arrest is not even the first instance of a wrongful arrest due to incorrect identification using facial recognition systems by the Detroit Police Department.[9] Individuals arrested and charged based on this incorrect identification are often subject to invasive processes of charge sheeting, fingerprinting, and questioning.[10] Their defense results in enormous expenses – only to prove that they are not the person accused of the crime.[11]

Given the trend in the United States of adopting facial recognition technology and other automated surveillance systems throughout both state and federal law enforcement,[12] cases like Williams' are becoming more common.[13] This is despite

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *See* Hill, *supra* note 1.

8. Jeremy Shur & Deborah Won, *The Computer Got It Wrong: Why We Are Taking the Detroit Police to Court over a Faulty Face Recognition "Match"*, ACLU (Apr. 13, 2021), https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match/; Timothy Williams, *Facial Recognition Software Moves from Overseas Wars to Local Police*, N.Y. TIMES (Aug. 12, 2015), https://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html.

9. Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime he Didn't Commit*, DETROIT FREE PRESS (Jul. 10, 2020, 11:42 AM), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/; *see also* Hill, *supra* note 1.

10. Rachel A. Harmon, *Why Arrest?*, 115 MICH. L. REV. 307, 311 (2016).

11. *See* Hill, *supra* note 1. These expenses can often result in thousands of dollars applied towards representation and other legal costs.

12. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-526, FACIAL RECOGNITION TECHNOLOGY: CURRENT AND PLANNED USES BY FEDERAL AGENCIES (Aug. 2021) [hereinafter "Facial Recognition Technology"].

13. Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV 552, 558 (2021) (discussing recent instances of law enforcement using facial recognition technology).

the fact that this technology has regularly been referred to by experts as "snake oil," because it is insufficient to establish the necessary probable cause for an arrest.[14] There are currently hundreds of private corporations offering solutions to law enforcement for conducting facial recognition, including, Clearview AI, Vigilant Solutions, and Rekognition by Amazon.[15] A common pitch these companies offer is that this technology will help reduce crime and terrorism, even though such claims are presumptuous at best and outright false at worst.[16] In addition to the high rate of false positives and false negatives, technology like this is frequently biased, resulting in a higher-than-normal false-positive rate for individuals on the basis of race.[17]

Yet, this has not served as a barrier for law enforcement.[18] Thousands of police departments and federal agencies have joined the fray in adopting facial recognition technology and other automated surveillance solutions.[19] They have resisted calls for accountability and oversight to monitor the usage of this technology.[20] In almost all instances, the executive agencies have adopted this technology without any legislative oversight.[21]

Cases like Williams' present a situation where an individual has been accused of a criminal act and has been arrested pursuant to an identification by such automated surveillance system.[22] In these cases, the police require a lawful warrant, barring situations where an exception may apply, to conduct a search or seizure under the Fourth Amendment.[23] To date, courts have not comprehensively explored the application of the Fourth Amendment to facial recognition technology and other automated surveillance technology.

14. Matthew Ivey, *The Ethical Midfield in Artificial Intelligence: Practical Reflections for National Security Lawyers*, 33 GEO. J. LEGAL ETHICS 109, 132 (2020).

15. Cameron Martin, *Facial Recognition in Law Enforcement*, 19 SEATTLE J. FOR SOC. JUST. 309, 313 & 325 (2020).

16. *Id.* at 312-13.

17. Claire Garvie & Laura M. Moy, *Face Surveillance in the United States*, AMERICA UNDER WATCH (May 16, 2019), https://www.americaunderwatch.com/.

18. *See infra* Section V.

19. *Id.*

20. Julie Bosman & Serge F. Kovaleski, *Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html ("several agencies have come forward to argue that it is counterproductive to forbid any use of what they call a valuable tool that generates investigative leads").

21. *Id.*

22. *See* Hill, *supra* note 1.

23. *See infra* Section I; Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the* Carpenter *Decision*, 16 OHIO ST. J. CRIM. L. 281 283-84 (2018).

*Fourth Amendment Constraints*

The Fourth Amendment has two specific requirements – (1) a warrant, and (2) probable cause.[24] This article addresses a specific facet of the Fourth Amendment probable cause clause, which is the requirement for particularity or specificity in the warrant.[25] When requesting a warrant, law enforcement is required to ensure that they particularly define (1) the place they expect to search, and (2) the person or things they expect to seize. While courts normally afford a degree of latitude in particularly defining the place, person, or things, the goal of the Fourth Amendment is to limit executive discretion.[26] It seeks to prevent general warrants, similar to the warrants used prior to the Revolutionary War by the erstwhile colonial British government, allowing the government to search through and rummage the information of dissidents without any limits.[27]

In addressing this issue, this article will establish that automated surveillance technology applied in public spaces must comply with the particularity requirement of the Fourth Amendment, since an individual continues to have a "reasonable expectation of privacy" requiring specificity when issuing a warrant.

This paper is divided into six sections. Section I analyzes the different theoretical foundations of the Fourth Amendment, particularly as they pertain to the right of privacy in the public.[28] Although historically the Fourth Amendment has not applied to whatever is in "plain view," there has never been a blanket prohibition on the Fourth Amendment's application in the public. Section II discusses the particularity requirement of the Fourth Amendment as identified through precedent.[29] It will explore the different dimensions of particularity identified by courts and their application to specific contexts. Further, it will also provide a brief overview of some statutory guidance used to supplement the requirements of the Fourth Amendment.

Section III explores automated surveillance technology and how it is distinct from traditional forms of surveillance.[30] The concept of traditional surveillance has expanded drastically and may even include technology like cameras. The distinction between traditional and automated surveillance technology is the lack of human oversight over automated surveillance technology. Section IV provides examples of automated surveillance technology used by law enforcement at both the federal

24. U.S. CONST. amend. IV; Martha Applebaum, *Wrong but Reasonable: The Fourth Amendment Particularity Requirement after* United States v. Leon, 16 FORDHAM URB. L. J. 577, 580 (1987).

25. U.S. CONST. amend. IV ("[N]o 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.").

26. Marshall v. Barlow's, Inc., 436 U.S. 307, 323 (1978) ("warrantless searches devolves almost unbridled discretion upon executive and administrative officers").

27. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); Marron v. United States, 275 U.S. 192, 195-96 (1927).

28. *See infra* Section I.

29. *See infra* Section II.

30. *See infra* Section III.

and state level in the United States.[31] Not only have police departments adopted this technology, but even agencies that traditionally have little to no law enforcement function have adopted automated surveillance technology.

Section V will analyze specific types of automated surveillance technology and how the particularity requirement applies in each of these contexts.[32] Important distinctions between real-time and manual facial recognition technology and specific problems created by automated surveillance technology such as aggregation, will be drawn. Section VI will provide recommendations on how courts and legislative bodies can address the existing gaps in Fourth Amendment jurisprudence relating to automated recognition technology and the particularity requirements, to ensure that the right to privacy in one's person is preserved in an age of rapidly advancing surveillance technology.[33] The article will conclude with a summary of how the Fourth Amendment limits the use of automated surveillance technology.[34]

## I. THEORETICAL FOUNDATIONS OF THE FOURTH AMENDMENT

The theoretical underpinnings of the Fourth Amendment provide an insight into the aims and objectives that sought to be achieved through its enactment.[35] They provide guidance on how the Fourth Amendment should be applied in different contexts to protect individual liberty, limit executive discretion, protect privacy interests, and determine when an individual's privacy interest is met. This section will also discuss the particularity requirement of the probable cause clause of the Fourth Amendment.

### *A. Limiting Executive Discretion*

Limiting executive discretion is one of the primary goals of the Fourth Amendment and probable cause clause.[36] The colonial British government would often enter an individual's private spaces to gather evidence necessary to incriminate them in court.[37] The judiciary, which itself operated at the interest of the King, was more

31. *See infra* Section IV.

32. *See infra* Section V.

33. *See infra* Section VI.

34. *See infra* Conclusion.

35. *See generally* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, UTAH L. REV. 977, 978 (2004) (the different models to measure reasonableness determine which forms of intrusions are permissible and which are not).

36. Marron v. United States, 275 U.S. 192, 195-96 (1927) (limiting executive discretion is the ultimate inquiry of the particularity requirement).

37. Applebaum, *supra* note 24, at 577; Steagald v. United States, 451 U.S. 204, 220 (1981).

than willing to accept this tainted evidence.[38] The Fourth Amendment aimed to change this dynamic.

The Fourth Amendment sought to prevent "general warrants" that allowed executive agencies to have unfettered discretion in rummaging through a person's home, papers, and effects, in addition to their person.[39] This purpose is where the particularity requirement of the Fourth Amendment plays a significant role. It requires law enforcement to specifically state what place is being searched and the items to be seized prior to the search itself.[40] The failure to specifically state this is sufficient to deny the warrant on the grounds of failing to demonstrate probable cause.[41] The purpose of particularity is to ensure that executive agencies do not have discretion when executing the warrant.[42] While there may be situations where executive agencies may need to exercise discretion, the particularity requirement generally operates with regard to a place, person, or thing.[43]

Executive discretion is deemed an evil that allows the government to operate unfettered and based on emotional impulses relating to a particular case.[44] The goal of including the judiciary in this process is to offer independent and impartial oversight of the criminal justice process.[45]

This desire to avoid executive discretion is also the reason why, since the twentieth century, the Fourth Amendment has steadily expanded to encompass new technology and dragnet-type surveillance that historically were never contemplated by the Founding Fathers.[46] A textual reading may have permitted the searches involved in several of these cases.[47] Through this process, principles such as the exclusionary rule and the "reasonable expectation of privacy" have developed to safeguard the protections traditionally afforded by the Fourth Amendment, yet have eluded a clear prescription in the law. As Justice Brandeis

38. Roger Roots, *The Framers' Fourth Amendment Exclusionary Rule: The Mounting Evidence*, 15 NEV. L.J. 42, 44 n. 12 (2014).

39. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

40. Maryland v. Garrison, 480 U.S. 79, 84-85 (1987) (quoting United States v. Ross, 456 U.S. 798, 824 (1982)).

41. Illinois v. Gates, 462 U.S. 213, 231 (1983).

42. *See supra* note 26.

43. U.S. CONST. amend. IV.

44. *Coolidge*, 403 U.S. at 467.

45. United States v. Jeffers, 342 U.S. 48, 51 (1951) ("the [Fourth] Amendment does not place an unduly oppressive weight on law enforcement officers but merely interposes an orderly procedure under the aegis of *judicial impartiality* that is necessary to attain the beneficent purposes intended") (emphasis added).

46. Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1455 (2004); United States v. Karo, 468 U.S. 705, 712 (1984); Kyllo v. United States, 533 U.S. 27, 31 (2001).

47. *See also* Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 241 (2019) (offering the example of textualism limiting the use of thermal imaging to search the effects of a person).

observed in *Olmstead v. United States*,[48] the Founders "conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men."[49]

Meanwhile, law enforcement has taken it upon itself to utilize automated surveillance technology like facial recognition. Over the past few decades, law enforcement throughout the country has received an enormous increase in funding, which has allowed a proliferation of new weaponry and technology to conduct law enforcement activities.[50] Law enforcement is increasingly using facial recognition for the purpose of identifying individuals and establishing probable cause for seeking a warrant. When law enforcement seeks a warrant, their potential use of this technology is not typically disclosed to the judiciary or the accused, limiting opportunities to sufficiently understand the implications of its usage and challenge the application in each case.[51] Additionally, its indiscriminate use has subjected the data of millions of people to the potential risk of cybersecurity breaches that can subject them to identity theft and other forms of digital crime.[52] Limiting executive usage of facial recognition technology and automated surveillance will further Fourth Amendment protections.

### *B. Protecting Privacy Interests in Person and Property*

Protecting privacy interests is deeply interlinked with the interest of limiting executive discretion in the process of establishing probable cause for searches involving individuals accused of crime.[53] Although the Fourth Amendment does not explicitly use the word "privacy", it has long been held as one of its fundamental purposes.[54] In one of the early Fourth Amendment cases, *Boyd v. United States*, the Court noted that it protected not only the home, but also "privacies of life."[55] While the Fourth Amendment has primarily been applied in the home and other private

48. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

49. *Id*.

50. *See generally* Garvie & Moy, *supra* note 17.

51. *Id.* at 13 (discussing difficulties with trying to obtain such data from various Chicago law enforcement entities).

52. *Id.*; *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-522, FACIAL RECOGNITIONS TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USE, 14 (2020) [hereinafter "Commercial Use"] ("[f]acial image data sets raise the same security concerns as those associated with any personal data– for example, they could be subject to data breaches, resulting in sensitive biometric data being revealed").

53. Note, *Protecting Privacy under the Fourth Amendment*, 91 YALE L.J. 313, 320 (1981).

54. *See* Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH. L. REV. 143, 157-62 (2015) (discussing reasons why privacy is an important concept to Fourth Amendment jurisprudence).

55. Boyd v. United States, 116 U.S. 616, 630 (1886).

spaces, there remains a question as to whether it applies in public.[56] The consensus today is that it does, albeit in a limited capacity.[57]

This right has been recognized regarding to directional information provided by cell phones, wiretapping, and the privacy interest oneself in public, which protects an individual from an unlawful search even in the public without establishing probable cause or an exception to the Fourth Amendment.[58] The goal of protecting an individual's privacy is to allow them to engage in the public effectively without fear of government reprisal.[59] Without such a limitation, an individual's characteristics would be subject to limitless scrutiny by the government. Exposing a person's intimate details would facilitate perverse incentives for both public and private individuals, who may seek to gather information about a particular individual for any number of reasons, related to law enforcement objectives or not.[60]

### *C. Reasonable Expectations of Privacy*

In the landmark case *Katz v. United States,*[61] fundamentally changed how Fourth Amendment searches are analyzed.[62] Historically, the Fourth Amendment would apply whenever law enforcement had committed a "trespass" on a person or their property.[63] The trespass standard was no longer workable in an age of technology, where police were listening to conversations through wiretapping. This resulted in the "reasonable expectation of privacy" standard, which solidified the role of the Fourth Amendment in preserving privacy.[64]

Despite this important step from the Court, its application the reasonable expectation of privacy to different technologies appears to be inconsistent, focusing

56. United States v. Knotts, 460 U.S. 276, 281 (1983) (explaining that traveling over public streets voluntarily conveys information to anyone who might be watching with the naked eye or with the assistance of technology); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986).

57. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018); United States v. Jones, 565 U.S. 400, 409-10 (2012).

58. Riley v. California, 573 U.S. 373, 385 (2014) (cell phones); Berger v. State of New York, 388 U.S. 41, 63 (1967) (wiretapping). *See generally* Lyle D. Larson, *End-Run Around the Fourth Amendment: Why Roving Surveillance is Unconstitutional*, 28 AM. CRIM. L. REV. 143 (1990). Directional information is any information that can be used to identify a person's movement, location, and speed, at various times.

59. *See generally Carpenter*, 138 S. Ct.

60. Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1115-26 (2021).

61. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

62. *Id*.

63. *Carpenter*, 138 S. Ct. at 2259. *Carpenter* recognized that there are two standards for determining whether a search took place under the Fourth Amendment. The first is when a physical trespass took place. The second is when there is a breach of a "reasonable expectation of privacy".

64. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *Carpenter*, 138 S. Ct. at 2213.

on the amount of information that is collected rather than the actual expectation of privacy.[65] For example, in *United States v. Knotts,*[66] the Court found that the use of radio signaling to track a vehicle in the public did not violate a reasonable expectation of privacy, since the individual had exposed themselves in public when driving their vehicle.[67] However, in a relatively similar situation identified in *United States v. Jones*,[68] the Court prohibited tracking using Global Positioning System (GPS) technology because of the extensive capacity it provided law enforcement to track an individual in granular detail, for long periods, and with little to no oversight.[69]

A similar interest is implicated in the use of automated surveillance technology. While police can normally observe a person in public, automated surveillance technology go a step further. It provides context and identification in a manner that exceeds the scope of a standard Fourth Amendment search.[70] It can immediately provide a person's identification, while at the same time continuously monitoring their activities, raising major question of its constitutional validity.[71] Of course, there are differences in how this technology is applied, which may render its application permissible in some circumstances.[72] It also raises questions of aggregation, wherein the data of millions of people are collected and stored remotely to run this type of automated surveillance technology.[73] This data can be cross-referenced without any concern for whether the individuals included in such databases are subject to any form of criminal investigation or other forms of legal liability.

The following sections explore some of the rationale for explaining how courts have applied the reasonable expectation of privacy standard, which is relevant for obtaining a warrant under the Fourth Amendment. They provide interesting insight into the Fourth Amendment and when the particularity requirement may need to be satisfied with reference to a specific technology.[74]

65. Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 975 (2012).

66. 460 U.S. 276.

67. *Id*. at 276-79.

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

69. *Id.* at 408-09, 429-30.

70. *Carpenter*, *supra* note 58, at 2209 (the Court referred to cell site location data collected on the continuous basis as "detailed, encyclopedic, and effortlessly compiled."); Doktor, *supra* note 13 at 567 (the Ninth Circuit "[cautioned] against facial recognition scans all real-time surveillance data[,]" comparing these type of scans to the cell site data being collected in *Carpenter*).

71. United States v. Donovan, 429 U.S. 413, 414 (1977).

72. *See infra* Section V.

73. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 514 (2006).

74. *See infra* Section I.C.1-4.

*Fourth Amendment Constraints*

*1. Probabilistic Model*

The probabilistic model of the Fourth Amendment stands for the proposition that where law enforcement would have uncovered information, notwithstanding a Fourth Amendment search, there might be a justification for conducting the search without a warrant.[75] For example, the plain view doctrine refers to situations where a particular item is exposed in plain view of the public on an individual's property. In such a case, this item would not receive Fourth Amendment protection.[76]

With automated surveillance technology, the probability that law enforcement may uncover particular information can vary significantly.[77] When an active investigation is being conducted to identify a particular individual, law enforcement may, in certain circumstances, have a reasonable probability of identifying the person and anticipate an arrest warrant in pursuance of such identification.[78] However, a large amount of surveillance is targeted towards people who are conducting lawful activities with limited interference from the public.[79] Automated surveillance technology may simply flag their activities in public when it perceives them to be acting in a behaviorally inappropriate manner.[80] For example, a system could flag an individual for public drunkenness or jaywalking.[81] In some states, these carry criminal penalties, often in the form of misdemeanors.[82] Police officers and members of the public will often choose to ignore such "crimes" due to the cost it would impose in enforcing and the practicalities of day-to-day interactions with the public.[83] On the other hand, automated surveillance technology may not be

75. Orin Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506 (2007).

76. Maryland v. Garrison, 480 U.S. 79, 86 n.3 (1987) (Blackmun, J., dissenting).

77. Kevin Macnish, *Unblinking Eyes: The Ethics of Automating Surveillance*, 14 ETHICS INFO. TECH. 151, 157, 163 (2012).

78. United States v. Mendenhall, 446 U.S. 544, 553-54 (1980).

79. Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, 35 CRIM. JUST. 7, 9–10 (2020).

80. Commercial Use, *supra* note 53 at 26; Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. LEGAL ANALYSIS 113, 131 ("when human behavior is involved, it can be extremely challenging to ascertain relevant motivations"); Catherine Crump & Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, BLOOMBERG LAW, (Aug. 21, 2012) https://www.bloomberglaw.com/bloomberglawnews/white-collar-and-criminal-law/X13RATL4000000?bna_news_filter=white-collar-and-criminal-law#jcite

81. *See e.g.*, Gabriel Hermosilla et al., *Face Recognition and Drunk Classification using Infrared Face Images*, J. SENSORS 1, 7 (2018). *See also* Matthew E Cavanaugh, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 MINN. L. REV. 2443, 2472 (2021) (providing an example of how CCTV is used more frequently to target minor crime rather than more serious crimes).

82. *See generally* David Keenan & Tina M. Thomas, *An Offense Severity Model for Stop-and-Frisk*, 123 YALE L.J. 1448, 1480 (2014).

83. Eric J. Miller, *Challenging Police Discretion*, 58 HOWARD L.J. 521, 521 (2015) ("[law] enforcement officials have tremendous discretion to determine the amount in style of policing that occurs in their jurisdiction. They decide what crimes or suspects to pursue, which communities or locations to target for policing, the best methods to prevent or respond to crime, and how best to balance prevention and detection.").

designed with this level of contextual awareness, resulting in possibilities of over-policing that have already proven to be true.[84]

Nonetheless, establishing the probability of whether law enforcement can gather information sufficient to establish probable cause is a tenuous discussion, which mostly takes place in the abstract.[85] The probabilistic model is useful in understanding the exceptions courts have developed for Fourth Amendment warrant requirements. These exceptions are discussed later in this section.

### *2. Private Facts Model*

The private facts model focuses on the intent of people.[86] It approaches the goals of the Fourth Amendment as the intent to keep certain information outside the purview of the public.[87] The protections of the Fourth Amendment extend to "persons, houses, papers, and effects."[88] However, the jurisprudence of the Fourth Amendment has allowed its impact to creep far beyond these boundaries, whether it is GPS tracking,[89] wiretapping,[90] roving surveillance,[91] geothermal imaging,[92] or cell phones.[93]

Identifying a privacy interest provides guidance as to the scope of the Fourth Amendment interest that needs to be protected.[94] With automated surveillance

84. Ngozi Okidegbe, *The Democratizing Potential of Algorithms?*, 53 CONN. L. REV. 741, 744 (2022) ("algorithmic governance reinforces and legitimizes the barriers that already impede their ability to challenge or to gain control over the criminal legal institution responsible for over surveillance, overcriminalization, and over-incarceration"); Joel R. McConvey, *Mistaken Arrest in Georgia Triggered by False Facial Recognition in Different States*, BIOMETRIC UPDATE (Jan. 3, 2023), https://www.biometricupdate.com/202301/mistaken-arrest-in-georgia-triggered-by-false-facial-recognition-match-in-different-state; Luke Stark & Jevan Hutson, *Physiognomic Artificial Intelligence*, 32 FORDHAM INTEL. PROP. MEDIA & ENT. L.J. 922, 960 (2022) ("AI systems and the racist logics underpinning their uses have already been responsible for mistaken arrests of Black citizens"); Jon Fingas, *Police Face Recognition Misidentified 2300 as Potential Criminals*, ENGADGET (May 6, 2018), https://www.engadget.com/2018-05-06-police-face-recognition-misidentified-2300-as-criminals.html (observing that South Wales Police in the United Kingdom had about 92% false positives, although no arrests based on the false positive).

85. T.J. Benedict, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849, 880-86 (2022).

86. Kerr, *supra* note 76, at 512.

87. *Id*.

88. U.S. CONST. amend. IV.

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

90. *Katz*, 389 U.S. at 359; *Berger*, 388 U.S. at 42–47.

91. *Berger*, 388 U.S. at 42–47.

92. *Kyllo*, 533 U.S. at 29.

93. *Riley*, 573 U.S. at 373–76.

94. Kerr, *supra* note 76, at 522-23.

technology, a person's movement in public can easily be observed by anyone.[95] Historically, an officer or member of the public can, under normal circumstances, observe a fellow human's movement in public without incurring any form of liability.[96] However, this does not mean that a person has no privacy interest in the public;[97] though diminished, an individual can reasonably expect to have a privacy interest in their person.[98] A similar logic applies regarding automated surveillance technology, given its ability to gather information far beyond what is normally available to members of the public, much of which can only be identified with prior knowledge of a particular person.[99]

*3. Positive Law Model*

The positive law model focuses on those privacy interests enshrined in statutory law.[100] This model would cover privacy interests that are widely protected, such as medical records, property interests, cell phone records, and banking information.[101] It is supplemented by the fact that the scope of the protected interest has received congressional or state legislative approval as deserving of protection from state intrusion.[102]

There are some states that have made inroads into regulating specific types of automated surveillance technology, with one of the most well-known statutory being the Illinois Biometric Information Privacy Act. This was enacted in 2008 in response to the growing use of biometric information in the information technology field.[103] It limits the collection, usage, safeguarding, handling, storage, retention, and destruction of "biometric identifiers."[104] This Act has served as a model, inspiring other states and municipalities to enact their own restrictions on biometric

95. Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1593 (2017).

96. United States v. Knotts, 460 U.S. 276, 281 (1983).

97. Robert P. Faulkner & Douglas H. Hsiao, *And Where You Go I'll Follow: The Constitutionality of Antistalking Laws and Proposed Model Legislation*, 31 HARV. J. ON LEGIS. 1, 39-40 (1994).

98. *Id.*

99. *Carpenter*, 138 S. Ct. at 2209 (the Court referred to cell site location data collected on the continuous basis as "detailed, encyclopedic, and effortlessly compiled."); Doktor, *supra* note 13 at 567 (the Ninth Circuit "[cautioned] against facial recognition scans all real-time surveillance data[,]" comparing these type of scans to the cell site data being collected in *Carpenter*).

100. Kerr, *supra* note 76, at 516.

101. *See* Whalen v. Roe, 429 U.S. 589, 603-04 (1977); *Carpenter*, 138 S. Ct. at 2,209-10.

102. Kerr, *supra* note 76 at 516 ("[if] the government broke the law in order to obtain the information it did, the government conduct violated a reasonable expectation of privacy.").

103. 740 Ill. Comp. Stat.

104. *Id.* §14/15.

surveillance and facial recognition technology by recognizing the dangers that facial recognition technology poses to individuals.[105]

*4. Policy Model*

The policy model recognizes that, as a matter of public policy, certain privacy interest need to be protected from the State in order to facilitate a robust criminal justice system and safeguard constitutional interests.[106] For example, protecting one's papers not only serves as a limit on executive discretion, but it also ensures that a person's personal preferences and ideas are not subject to a chilling effect where the State can simply infringe upon a person's thoughts by entering into a protected space.[107] Policy is a subjective basis upon which to establish privacy rights, especially those related to the Fourth Amendment; however, this model usually serves as a supplement for arguing the existence of any privacy interests,[108]

In the context of facial recognition technology, while an individual undoubtedly has a privacy interest in their biometric information, the extent of this interest is questioned frequently.[109] When in public, a person's face is visible. Does the application of facial recognition technology render the protections of the Fourth Amendment inert merely because the interest traditionally would not have been protected to the same extent in public? From a policy standpoint, a person's interest in their face concerning facial recognition technology affects and goes beyond mere observation.[110] To avoid constant surveillance resulting in a chilling of expression, limiting of individual activity, and policing people based on non-criminal offenses, there is a need to limit surveillance of the public.[111] The failure to recognize any protections against such forms of surveillance would, in effect, infringe upon multiple constitutional rights and undermine democratic institutions and social relations.

105. Stacy Norris, *". . . and the Eye in the Sky Is Watching Us All" - the Privacy Concerns of Emerging Technological Advances in Casino Player Tracking*, 9 UNLV GAMING L.J. 269, 284 (2019). Illinois was the first state to recognize a private right of action against companies that used facial recognition technology in contravention with the law. This has inspired many other states, including Texas and Washington, to enact similar laws.

106. Kerr, *supra* note 76, at 521.

107. Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. & MARY L. REV. 1,633, 1673-74 (2013).

108. Kerr, *supra* note 76, at 519.

109. Hirose, *supra* note 96 at 1600-08 (discussing how courts have grappled with the privacy interests of a person including their physical characteristics); Jennifer Lynch, Face-Off: Law Enforcement Use of Face Recognition Technology, Elec. Frontier Found. (2018), https://www.eff.org/wp/law-enforcement-use-face-recognition (the privacy concerns implicated by using facial recognition are even more serious than using other forms of identification because the face cannot be changed).

110. Hirose, *supra* note 96 at 1608.

111. Kendrick, *supra* note 108, at 1674.

### *D. Exceptions where Privacy Expectations Are Limited*

There are a limited number of exceptions to the Fourth Amendment,[112] allowing law enforcement to conduct searches without either meeting the probable cause standard or seeking a warrant.[113] Where one of the exceptions applies, the implicated privacy interest is lowered through judicial intervention.[114] The following section will briefly review these exceptions to provide jurisprudential context to the Fourth Amendment and highlight how the Fourth Amendment might interact with automated surveillance technology.[115]

#### *1. Third-Party Doctrine*

The third-party doctrine is one of the most frequently invoked doctrines regarding emerging technology and the Fourth Amendment.[116] The doctrine provides that an individual who shared information voluntarily with a non-governmental third party, , can have that information seized by law enforcement, who can then bypass the individual and directly request the information from the third-party.[117] In such cases, the usual standards for a warrant and probable cause need not be met.

It was first invoked in the case of *United States v. Miller*,[118] where the local police requested banks to provide records of a criminal organization accused of smuggling alcoholic beverages.[119] The Court found there was no legitimate expectation of privacy with regard to seizing the bank records by virtue of the third-party doctrine.[120]

In the age of digital information, potential limitations on the third-party doctrine's otherwise-unilateral application have arisen. With the recent case *Carpenter v. United States*, the Supreme Court considered the application of the third-party doctrine to tracking information collected from a telecommunication

112. People v. Nunes, 278 Cal. Rptr. 3d 425, 428 (Ct. App. 2021) ("Recognized exceptions to the general rule against warrantless home searches must be narrowly construed to prevent the exceptions from swallowing the important Fourth Amendment right." (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 454 (1971))).

113. *Id.* at 454-55.

114. Leslie A. Harasym, *Drug Testing and the Fourth Amendment*, 2 J. CIV. RGHTS. & ECO. DEV 1, 5-6 ("exceptions have been carved out where the intrusion seems reasonable"); Brian J. Serr, *Greater Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 608 n.113 (1989) ("lower expectation of privacy associated with automobiles.").

115. *See infra* Section II.D.1-3

116. Alan Z. Rozenshtein, *Fourth Amendment Reasonableness after* Carpenter, YALE L.J. FORUM 943, 944 (2019).

117. *Id.*

118. United States v. Miller, 425 U.S. 435 (1976).

119. *Id.* at 436-37.

120. *Id.* at 442-43.

agency about the movements of the accused.[121] Law enforcement used the information they collected to develop a comprehensive map of information of where the accused moved during the time of investigation, virtually in real-time. The Court noted that the collection of a person's movement and location is "a[] … different species of business record" – one that implicates Fourth Amendment concerns.[122]

*Carpenter* represents one of the first cases that changes the standard by which the third-party doctrine could be applied and suggests that the third-party doctrine may not unilaterally defeat a claim of privacy going forward, as it had since its inception. While the Court required its opinion to be construed "narrowly," the potential implications for emerging technology are clearly developing.[123]

### *2. Community Caretaking*

The community caretaking exception allows courts to weigh the reasonableness of law enforcement actions by balancing the public interest and an individual's reasonable expectation of privacy. It was first established in *Cady v. Dombrowski*, where the Court allowed a warrantless search of a person's vehicle following an accident that led to the identification of a revolver in the accused's possession.[124] However, this exception is narrowly construed, and recent cases have refused to expand its scope.[125]

The exception presents interesting problems regarding automated surveillance technology, because of the potential blanket protections it could afford to law enforcement agent if they were granted immunity on this basis for failing to adhere to the requirements of the Fourth Amendment.[126] Specifically, it would allow for widespread surveillance without independent oversight, which could change the dynamic of individual rights across the country.[127]

121. 138 S. Ct. 2206, 2216 (2018).

122. *Id.* at 2222.

123. *See id.* at 2220 ("[o]ur decision today is a narrow one.").

124. 413 U.S. 433, 448 (1973).

125. Caniglia v. Strom, 141 S. Ct. 1596, 1599 (2021) (rejecting the First Circuit's expansion of the "community caretaking" exception); Colorado v. Bertine, 479 U.S. 367, 381 (1987) (Marshall, J., dissenting) ("[standardized] procedures are necessary to ensure that this *narrow exception* is not improperly used to justify . . . a warrantless investigative foray" referring to the community caretaking exception) (emphasis added).

126. *See* Brief of Project for Privacy & Surveillance Accountability and Restore the Fourth, Inc. as Amici Curiae Supporting Petitioner at 17-20, Caniglia v. Strom, 141 S. Ct. 1596 (2021) (No. 20-157) [hereinafter "Privacy and Surveillance Accountability"] (explaining that "[i]f the Court extended the community-caretaking exception to the home," the government would have greater discretion to expand the area of warrantless searches without violating the Fourth Amendment).

127. *Id.*

*3. Good Faith*

The good-faith exception to the Fourth Amendment applies when law enforcement received a faulty warrant, whether for a search or seizure.[128] It in practice legitimizes any search conducted in pursuance of a warrant if the officers acted in "good faith" when executing in a warrant.[129]The good-faith exception operates post-search that is after the officers had reasonably relied on the warrant. Searches that are otherwise illegal under the Fourth Amendment can still receive *ex post* judicial approval of the search, considering them as though it had been valid from the start.[130]

## II. FOURTH AMENDMENT PARTICULARITY REQUIREMENTS

The particularity requirement of the Fourth Amendment is created by the probable cause clause, which supplements the warrant requirement of the Fourth Amendment.[131] It requires that law enforcement particularly describe the "places to be searched" and "things to be seized" before a warrant can be granted.[132] It prohibits warrants that are "general, exploratory rummaging in a person's belongings."[133] Generally, courts require that there be a highly particular description of the place to be searched and things to be seized to satisfy this requirement, although law enforcement is normally afforded some degree of latitude.[134]

128. *See e.g.*, United States v. Leon, 468 U.S. 897, 922-23 (1984) (holding that the costs of excluding evidence obtained when using a "subsequently invalidated search warrant" does not justify the minimal benefits defendants obtain through the suppressing of evidence); Thomas M. Harrison, Note, *Good Faith and the Particularity-of-Description Requirement*, 53 MO. L. REV. 355 n.2 (1988).

129. *See* Harrison, *supra* note 93, at 355 n.2.

130. *See infra* Section VI. The good faith doctrine is useful when conceptualizing different judicial and legislative instruments that have expanded or contracted Fourth Amendment protections vis-à-vis governmental power. It can be understood alongside remedies available for violations of the Fourth Amendment, as a "pseudo-remedy" for state agencies that failed to meet the specific requirements of the Fourth Amendment.

131. Applebaum, *supra* note 24, at 577 & n.1; *see also* U.S. CONST. amend. IV ("no [w]arrants shall issue, but upon probable cause … and particularly describing the place to be searched, and the persons or things to be seized.").

132. U.S. CONST. amend. IV.

133. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

134. Bernadette Turi Romano, *Is the New Standard for the Fourth Amendment Particularly Requirement in Obscenity Cases "I Know It When I Seize It"?*, 39 SYRACUSE L. REV. 1113, 1132-36 (1988) (discussing how strictly applying the particularity requirement may not even be feasible and may require balancing policy considerations).

### *A. The Requirements of Particularity*

The requirements for particularity when seeking a warrant are not extensive.[135] Particularity is determined on a case-by-case basis to limit executive discretion and provide sufficiently precise language informing the officer how to separate items that are properly subject to seizure.[136] Courts normally consider whether probable cause existed to support the seizure of all or some of the items described in the warrant.[137] Courts also place a significant emphasis on the nature of the crime and the evidence sought, where serious crimes of great urgency receive a discretionary latitude when particularly defining the search or seizure to be executed.[138]

In addition to the particularity of the terms for search or seizure, courts have emphasized spatial and temporal dimensions of particularity, which limit the space that law enforcement can search based on probable cause and the amount of time for which the search can be conducted, respectively.[139] These requirements are applicable to both things and persons.[140] Although there is no bright-line rule, broad searches with few limits are found to violate the Fourth Amendment. For example, courts have noted that a warrant allowing for wiretapping communications over two months without any limit lacked particularity.[141]

The particularity requirement does not apply to the method of executing the warrant, which courts have held remain in the discretion of law enforcement.[142] It only applies to the places, persons and things being searched and seized, respectively.[143]

### *B. Particularity in Specific Contexts*

Privacy interests are implicated in a wide variety of contexts that courts have adjudicated since the enactment of the Fourth Amendment.[144] This section explores Fourth Amendment particularity with reference to cases discussing privacy interests, including some cases that focus on the privacy interests in public spaces.

135. *See generally* Applebaum, *supra* note 23, at 580–589 (noting the factors used to determine whether warrant particularity is met for both places and property).

136. Applebaum, *supra* note 24, at 580 (citing Marron v. United States, 275 U.S. 192, 196 (1927)).

137. Applebaum, *supra* note 24, at 580 (citing Maryland v. Garrison, 480 U.S. 79 (1987)).

138. Applebaum, *supra* note 24, at 580 (citing United States v. Cook, 657 F.2d 730, 733 (5th Cir. 1981)).

139. Steele v. United States, 267 U.S. 498, 503 (1925) (particularity of the place); Berger v. New York, 388 U.S. 41, 59 (1967) (temporal limitations).

140. U.S. CONST. amend. IV.

141. *Berger*, 388 U.S. at 59.

142. United States v. Chadwick, 433 U.S. 1, 7, 9 (1977).

143. United States v. Leon, 468 U.S. 897, 906 (1984).

144. *See* Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 111 (1988) (discussing some of the Supreme Court's most recent Fourth Amendment opinions and their implications for privacy interests).

Some of the first cases to review particularity dealt with wiretapping.[145] These cases, *Katz* and *Berger v. New York*, signaled that both spatial and temporal particularity was important as a factor in determining the scope of privacy rights.[146]

In this vein, courts have held that roving surveillance, involving surveilling an individual across multiple locations and different times, is not permissible due to a lack of particularity, except in situations where law enforcement lacks any reasonable alternatives.[147] Yet at the same time, courts have recognized that information in plain view of the public is not subject to Fourth Amendment protections.[148] An extension of the plain view doctrine is in the context of vehicles, which have a lower expectation of privacy, one of the reasons being that they move in the view of the public.[149]

Over the course of several decisions courts have recognized limits on geothermal surveillance,[150] cell phone searches,[151] drug-dog sniffing,[152] and the use of cameras in nonpublic spaces.[153] Although the jurisprudence is somewhat inconsistent, repeated themes deemed relevant by the court the amount of information collected. This helps determine the privacy interest of the public and the ability of law enforcement to collect information through other less intrusive means.[154]

## III. AUTOMATED SURVEILLANCE TECHNOLOGY

An individual's face is always exposed to the public. Accordingly, under a traditional understanding of the Fourth Amendment, facial and other bodily characteristics are unlikely to be protected.[155] However, automated surveillance technology changes this by providing more than can be gleaned through observation by the naked eye. Much of this technology can provide encyclopedic levels of information about a

145. *Katz*, 389 U.S. at 348; *Berger*, 388 U.S. at 45.

146. *See Katz*, 389 U.S. at 355 (holding that a concealed electronic device can only be deployed for the "narrow and particularized" purpose stated in the warrant); *Berger*, 388 U.S. at 55-56.

147. *Berger*, 388 U.S. at 59.

148. Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 26 (2013) (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).

149. Chambers v. Maroney, 399 U.S. 42, 48 (1970) ("the Court [in Carroll] held that automobiles and other conveyances may be searched without a warrant in circumstances that would not justify the search without a warrant of a house or an office, provided that there is probable cause to believe that the car contains articles that the officers are entitled to seize.").

150. *Kyllo*, 533 U.S. at 29.

151. *Riley*, 573 U.S. at 378.

152. Florida v. Jardines, 569 U.S. 1, 11–12 (2013).

153. *See* United States v. Torres, 751 F.2d 875, 876, 878 (7th Cir. 1984).

154. *See supra* Section II.B.

155. *See* Jace C. Gatewood, *District of Columbia Jones and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504, 514 (2014).

particular individual.[156] Take facial recognition technology, a pervasive form of automated surveillance technology: (1) it can provide information about a person's physical characteristics, like their height, weight, appearance, and other identifying traits; (2) it can provide demographic information about an individual, like their race, gender, ethnicity, age, disability, and familial status; (3) it can provide behavioral attributes, like criminal activity, health care status, intent and emotion; and (4) it can provide information about an individual's travel direction, speed, and location.[157] While this technology is by no means limited to providing this information, it provides just a small glimpse into the enormous capabilities of this technology: , it can analyze contextual factors that the system has either been programmed to interpret or has learned itself through supervised or unsupervised machine learning, where an average human would be unable to do so.[158]

The dangers of automated surveillance technology are immediately apparent. The following section analyzes what "surveillance" means, and what constitutes the subcategory of "automated surveillance."[159]

### *A. Traditional Surveillance Systems*

Surveillance broadly refers to monitoring a scene concurrently with behavior analysis of people, for the purpose of maintaining security or keeping a watch over an area.[160] Traditional forms of surveillance have included standard searches by police officers, wiretapping, seizure of papers and effects, and searching an automobile, just to name a few examples.[161] Such forms of surveillance often require a human to monitor the communication or require the communication to be archived, so that it can later be examined by a human.[162]

Some of these forms of surveillance have been subject to a traditional Fourth Amendment analysis, which involves trespass into an individual's person or property.[163] Others have applied a reasonable expectation of privacy standard, wherein law enforcement usually monitors the individual or their associates using specific technology.[164]

156. *See id.* at 512.

157. Ferguson, *supra* note 63 at 1110-11, 1119-20, 1122-23 (2021).

158. *See id.* at 1111-12.

159. *See infra* Section III.A.

160. ENCYCLOPEDIA OF BIOMETRICS 1309 (Stan Z. Li & Anil K. Jain eds., 2009).

161. *See id.*

162. Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 3 (2022) ("persistent surveillance is distinguishable from traditional surveillance . . . [is the] non-human, machine technology being used").

163. *Jardines*, 569 U.S. at 5-6.

164. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

### *B. Automated Surveillance Systems and Behavioral Biometrics*

Automated surveillance is surveillance with no or minimal human intervention involved in the processing and usage of the surveillance data collected.[165] This type of surveillance can take many forms, the most common being biometrics.[166] Biometric automated surveillance involves the analysis of physical characteristics of an individual, which can include their face, fingerprints, retinal scans, and voice identification.[167]

Automated surveillance has many distinct categories and problems associated with its application, which include facial recognition – a common form of automated surveillance.[168] Facial recognition can primarily be split into two sub-categories: real-time and manual.[169] Manual facial recognition operates with some degree of human intervention, primarily in triggering the application of the facial recognition.[170] Usually, a human agent will input data that needs to be cross-referenced across a facial recognition database, which will produce an output identifying faces that are similar to the inputs.[171] On the other hand, real-time surveillance is used in a dragnet fashion, where individuals who cross a sensor that is part of the surveillance network, such as a camera, will be identified and categorized automatically.[172]

The system can perform a wide variety of analyses. At its most basic level, the goal is to identify an individual.[173] However, many systems also have the ability to detect behavioral characteristics, such as when an individual is attempting to commit a crime or disrupt public activities.[174] This leads to situations where

165. ENCYCLOPEDIA OF BIOMETRICS, *supra* note 122, at 1309.

166. *Id.*

167. *Id.*

168. Monika Zalnieriute, *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, 22 COLUM. SCI. & TECH. L. REV. 284 (2021) (acknowledges that facial recognition technology can be a form of automated surveillance); Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020) ("proposals to curb or ban some uses of automated surveillance tools, including facial recognition software").

169. *See* Hirose, *supra* note 96 (explaining how governments may use real-time facial recognition technology); Kerri A. Thompson, *Countenancing Employment Discrimination: Facial Recognition in Background Checks*, 8 TEX. A&M L. REV. 63, 71 (2020) ("[e]arly facial recognition systems were not automated and required manual input"); *see e.g.*, Accountability, *infra* note 180 at 7 (Clearview AI claims that its software is "not for real-time surveillance"). Manual facial recognition refers to any system that is not real-time.

170. Thompson, *supra* note 168 at 71.

171. *Id.*

172. *See* Hirose, *supra* note 96 at 1596 (explaining how real-time facial recognition surveillance operates).

173. *See* Rebecca Darin Goldberg, Note, *You Can See My Face, Why Can't I? Facial Recognition and* Brady, 5 COLUM. HUM. RTS. L. REV. 261, 272 (2021).

174. *See* Hirose, *supra* note 96 at 1596 (explaining how systems can detect behavior); Christopher Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs*, NAT. INST. JUST. 3-5 (2019),

automated surveillance technology makes determinations based on data that it has been trained on.[175] In situations where the data is flawed, corrupted, or biased, the output of the system may reflect these biases.[176] Research has shown that many automated surveillance systems have inherent biases based on race and gender, in addition to the inability to consider cultural factors that may lead to flawed outcomes in different contexts.[177] Cultural factors may differ on a state-by-state basis, resulting in varied levels of false positives.[178]

## IV. INSTANCES OF AUTOMATED SURVEILLANCE IN THE UNITED STATES

To highlight the need to identify the applicability of the Fourth Amendment to automated surveillance technology, this section provides an overview of how federal and state agencies throughout the country are using automated surveillance technology with little to no oversight.

### *A. Federal Agencies*

There is extensive usage of facial recognition technology and automated surveillance by federal agencies. In two separate surveys conducted by the Government Accountability Office ("GAO"), nineteen and twenty agencies, respectively, reported using facial recognition technology for a wide variety of purposes.[179] While not all of them used the technology for law enforcement purposes, all reported using the technology for surveillance.[180] The Federal Bureau

https://www.ojp.gov/pdffiles1/nij/252038.pdf ("developing algorithms to identify actions such as traffic accidents and violent crime").

175. *See* Vivian D. Wesson, *Why Facial Recognition Technology is Flawed*, N.Y. STATE BAR ASS'N: BAR JOURNAL (July 7, 2020), https://nysba.org/software-isnt-magic-facial-recognition-technology-needs-reform/ (discussing how technology develops biases based on the data on which it was trained); Thompson, *supra* note 170, at 74 (2020).

176. Alice Xiang, *Reconciling Legal and Technical Approaches to Algorithmic Bias*, 88 TENN. L. REV. 649, 657-58 (2021).

177. *See* Thompson, *supra* note 170 at 73-75 (discussing higher than average error rates in facial recognition among some demographics).

178. *See generally* Pak-Hang Wong, *Cultural Differences As Excuses? Human Rights and Cultural Values in Global Ethics and Governance of AI*, 33 PHIL. & TECH. 705 (2020) (discussing the impact cultural differences may have on AI governance).

179. *See* Facial Recognition Technology, *supra* note 12, at 9–10 (identifying nineteen government agencies using facial recognition technology); U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-518, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCY SHOULD BETTER ASSESS PRIVACY AND OTHER RISKS 8, 17-20 (2021) [hereinafter "Accountability"] (identifying twenty government agencies using facial recognition technology and the various uses of the technology).

180. *See* Facial Recognition Technology, *supra* note 12, at 51, 56 (explaining the uses of facial recognition technology); Accountability, *supra* note 180, at 1, 7, 17, 19 (explaining the uses of facial recognition technology)..

of Investigation ("FBI"), which is a significant user of facial recognition technology, claims not to use real-time surveillance.[181] To develop the facial recognition technology, the FBI collected data – like passports – from international sources, states, and federal databases like passports, in order to develop a database of 640 million unique images of individuals.[182] Although the FBI database is immense, it is dwarfed in comparison to the Clearview AI database, which contains over 3 billion images from sources all over the world, and is one of the largest databases developed by either public or private entities.[183]

The analysis provided by the FBI facial recognition system is frequently used to gain leads on investigations.[184] The FBI admitted that they did not use the technology to establish probable cause, only to follow up and gather further evidence.[185] The FBI has teams dedicated to vetting the information output before it is shared with any other entity to ensure that the match is accurate.[186] The FBI claims it provides states with information of only one identified individual, under the pretense that it is to protect the privacy of individuals.[187]

The GAO provided a series of recommendations in 2016 to ensure accountability in the use of facial recognition technology, which as of 2021 the FBI has only partially adopted.[188] These include conducting privacy impact assessments, reviewing privacy standards, conducting annual audits, providing guidelines for the usage of facial recognition, and running constitutional impact assessments.[189]

181. *See Law Enf't's Use of Facial Recognition Tech: Hearing Before the H. Comm. on Oversight and Gov't Reform,* 115th Cong. 76, 124 (2017) [hereinafter "FBI Committee Hearing"] (discussing the breadth of the FBI's facial recognition use).

182. Neema Singh Guliani, *The FBI Has Access to over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through; *Facial Recognition Technology: Part II Ensuring Transparency in Government Use Before the House Oversight and Reform Committee,* 116th Cong. 21, 16 (2019), https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Transcript-20190604.pdf [hereinafter "FBI Congressional Hearing"] (statement of Kimberly J. Greco, Deputy Assistant Director of FBI) ("[our] system doesn't capture real-time. A probe photo has to be submitted to the [system] by law enforcement, and they have to have authority to access our system for a law enforcement purpose").

183. *See* Accountability*, supra* note 180, at 15-16 (comparing the FBI's facial recognition technology database to that of Clearview AI).

184. FBI Congressional Hearing, *supra* note 183 at 4.

185. *See* FBI Committee Hearing, *supra* note 182, at 3 (explaining how federal agencies use facial recognition technology without having probable cause).

186. *Id.* at 115.

187. *See id.* at 6, 128 (discussing how the FBI collects and retains the identities of identified individuals).

188. Accountability, *supra* note 180, at 1 n.1.

189. U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACIAL RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 34 (2016).

On the other hand, the Department of Homeland Security ("DHS") and Customs and Border Protection ("CBP") use real-time surveillance.[190] These agencies are encouraged and have run privacy impact assessments and reviewed privacy standards before using the technology.[191] The agencies allege that any information collected during surveillance is deleted from their systems within fourteen days, unless necessitated by further investigative requirements.[192]

In addition to this, the remaining federal agencies conduct a wide variety of activities using facial recognition for purposes ranging from cybersecurity to crime prevention and border protection.[193] In all of these cases, there is no explicit congressional directive allowing for the usage of facial recognition technology, though in almost all of these cases, the agencies recognized statutory obligations to maintain the privacy of the data collected.[194] Many federal agencies use private solutions to conduct facial recognition.[195]

### *B. State Agencies*

Many states use automated technology, but this is often utilized in secret.[196] States and municipalities have shirked their responsibility to the public to a greater degree.[197] Many states have deployed automated surveillance technology and facial recognition without any legislative approval.[198] In some states, police departments

190. Accountability, *supra* note 180 at 49, 54; *see* also Facial Recognition Technology, *supra* note 12, 52-53.

191. Accountability, *supra* note 180 at 3 ("if an agency reported having a system in operation, we requested privacy impact assessments"); *see e.g.*, *U.S. DEP'T OF HOMELAND SEC.*, *ICE Use of Facial Recognition Services*, DHS/ICE/PIA-054 (2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

192. U.S. CUSTOMS & BORDER PROT., *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport* (Nov 10, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint; *Federal Law Enforcement Use of Facial Recognition Technology*, CONG. RSCH. SERV., 14–15 (2020), https://sgp.fas.org/crs/misc/R46586.pdf.

193. *Id.*

194. Barry Friedman & Andrew Guthrie Ferguson, Opinion, *Here's a Way Forward on Facial Recognition*, N.Y. TIMES (Oct. 31, 2019), https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html ("Federal agencies have no clear democratic mandate nor any explicit legislative authority to use facial recognition"); *see also* John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition*, 25 HASTINGS COMMC'N. & ENT. L. J. 65, 73 (2002).

195. Accountability, *supra* note 180, at 7.

196. Abdullah Hasan, *2019 Proved We Can Stop Face Recognition Surveillance*, ACLU (Jan 17, 2020), https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable (" . . . federal and local law enforcement agencies have been eagerly adopting this technology too, often in secret"); *see* FBI Committee Hearing, *supra* note 139, at 76-77.

197. *See generally* Garvie & Moy, *supra* note 17.

198. Georgetown Law, Half of All American Adults are in a Police Face Recognition Database, New Report Finds (2016), https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds/ ("[of] the 52 agencies that acknowledged using face recognition, only one obtained legislative approval for its use")..

of specific counties and cities have adopted automated surveillance technology without any approval from the state legislature or executive agencies.[199]

Currently, one in four police departments that have adopted or have access to some form of facial recognition technology.[200] Most of the systems used by state entities are private solutions that are often used without any further refining or training, which is usually needed to improve the accuracy of the systems.[201] The solutions are often available "off-the-shelf" for any law enforcement agency in any state to purchase.[202] They simply require the funding to purchase this technology, which is often provided through funding allocated either by the state or federal government, both of which make significant contributions to police departments throughout the country.

The Detroit Police Department, which arrested Robert Williams based on a false-positive produced by these facial recognition systems, extensively uses facial recognition.[203] In Detroit alone there are two other recorded incidents of false-positives.[204] Despite this, law enforcement in Detroit has far from limited their use of facial recognition and other forms of automated surveillance.[205] In fact, Detroit and Chicago have adopted real-time surveillance facial recognition technology,

199. *Id.*

200. Georgetown Law, *supra* note 199; *see also* Clare Garvie, *The Perpetual Line-Up*, CTR. PRIVACY & TECH, GEORGETOWN LAW (Oct 18, 2016), https://www.perpetuallineup.org/ ("FBI should refrain from searching driver's license and ID photos in the absence of express approval for those searches from a state legislature").

201. Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, N.Y. Univ. Ctr. for Catastrophe Preparedness & Response (2009), http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

202. *See* Kashmir Hill, *Activists Turn Facial Recognition Tools Against the Police*, N.Y. TIMES (Oct 21, 2022), https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html ("activists say it has become relatively easy to build facial recognition tools thanks to off-the-shelf image recognition software") (discussing the use of solutions like Clearview AI); Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (Apr 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ ("[government] agencies often purchase or license facial recognition software from private companies").

203. Amy Harmon, *As Camera's Track Detroit's Residence, a Debate Ensues over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html ("facial recognition program matches the faces picked up across the city against 50 million driver's license photographs"); Garvie & Moy, *supra* note 17 (discussing project that dramatically increased surveillance cameras in Detroit); *supra* note 1.

204. Thompson, *supra* note 170, at 70.

205. *See generally* Garvie & Moy, *supra* note 17. Detroit paid more than $1 million over three years to develop their facial recognition technology infrastructure beginning in 2017. This system supports over 100 concurrent feeds that provide real time surveillance. Along with this, public-private initiatives in the city have helped provide a robust network of high-definition security cameras throughout the city. As a result, Detroit has leveraged their public resources and the private interest in safety to develop a network of cameras that provide a means for vast facial recognition; FBI Congressional Hearing, *supra* note 183 at 37.

being among the first government agencies in the United States to do so.[206] Unlike manual facial recognition, where an officer would need to input an image to get a result, real-time surveillance can be deployed across a network of Closed-Circuit Television (CCTV) cameras and other dragnets that can allow for continuous surveillance of the public.[207] These are some of the most intrusive types of surveillance currently available, as it exposes people to highly intrusive monitoring on a constant basis without any limits, providing law enforcement with immense amount of information without traditional due process protections that would have existed without this technology.

In a similar context, the Baltimore Police Department has also started a system of aerial surveillance, where an aerial vehicle is flown over the city several times a day carrying a camera that can take images of thirty-two square miles per second, which is then uploaded to a ground station that process the images and conducts surveillance.[208] This type of system was recently struck down by a court on the grounds that it violated the Fourth Amendment, a decision that was sustained on appeal.[209]

Despite a large number of law enforcement users of this technology, only a handful of states have any law that regulates the use of facial recognition and any of the ancillary effects that the technology will have on the public.

## V. CONTEXTUAL APPLICATION OF THE FOURTH AMENDMENT

There are different types of automated surveillance technology that can affect an individual's personal freedoms. This section addresses the use of technology like facial recognition, categorizes the different types of automated surveillance technology, and the problems that arise through its use. The application of this technology affects the extent to which Fourth Amendment interests are implicated.[210] Accordingly, this section will analyze the Fourth Amendment's applicability with reference to automated surveillance technology that conducts passive searches and real-time searches, involves data aggregation, and uses automated analysis.

206. *See generally* Garvie & Moy, *supra* note 17; FBI Congressional Hearing, *supra* note 183 at 37.

207. *See generally* Garvie & Moy, *supra* note 17.

208. Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 333 (4th Cir. 2021).

209. *Id.*

210. *See infra* Section V.A-D.

## *Fourth Amendment Constraints*

### *A. Passive Search*

Passive searches are the most frequently used method of automated surveillance technology, particularly with reference to facial recognition.[211] They involve law enforcement agencies gathering information about an individual or group and running that information through an automated surveillance technology system to gain insights to further an investigation or establish probable cause.[212]

Most agencies across the country utilize passive search in their facial recognition technology.[213] The FBI, a prominent user of facial recognition technology uses passive search in their investigations.[214] Annually, the FBI conducts over 150,000 searches on images provided by federal and state agencies to identify individuals.[215] It claims that these searches do not implicate constitutional rights. The FBI's stance that these searches implicate a lower privacy expectation is supported by the government's existing practice of identifying an individual through similar technologies.[216] People already submit their identification information to the government, which is then searched by other government agencies.[217] A simple showing of probable cause by identifying the individual and the associated crime may be sufficient in order to run this type of search.[218]

However, using automated surveillance technology to gather more information beyond pure identification may implicate additional concerns under the Fourth Amendment.[219] The nature of the information being sought and the reasons for conducting such a search would need to be analyzed on a case-by-case basis depending on the specific technology being applied, thereby establishing specificity

211. Harold Laidlaw, *Shouting Down the Well: Human Observation as a Necessary Condition of Privacy Breach, and Why Warrants Should Attach to Data Access, Not Data Gathering*, 70 N.Y.U. ANN. SURV. AM. L. 323, 362 (2015). Passive searches referred to situations where automated surveillance technology is applied to individual information, whether that person has been identified or not, to conduct analysis on any number of factors that include identification, geographic location, or even intend analysis. It normally is applied by law enforcement once some information is gathered about an individual who is accused of committing a crime or other civil offense and conducting analysis using the information gathered. For example, an individual accused of stealing from a grocery store may be caught on CCTV camera. Law enforcement may use the images from the CCTV to identify the individual by running the images through a facial recognition system.

212. FBI Congressional Hearing, *supra* note 183 at 37 ("[the FBI] system doesn't capture real-time") (discussing how a probe photo has to be submitted).

213. FBI Committee Hearing, *supra* note 182 at 11.

214. FBI Congressional Hearing, *supra* note 183 at 37 ("[the FBI] system doesn't capture real-time") (discussing how a probe photo has to be submitted).

215. FBI Congressional Hearing, *supra* note 183 at 21.

216. United States v. Donovan, 429 U.S. 413, 423 (1977) (finding a need for particularity and probable cause even though identification is a legitimate government purpose with few exceptions).*See* Gonzalez v. Immigration and Customs Enforcement, 975 F.3d 788, 822 (9th Cir. 2020).

217. *Donovan*, 429 U.S. at 423 (1977).

218. *Id.* at 420–21.

219. Hirose, *supra* note 96, at 1595.

for the crime in question.[220] Factors that should be considered when running such forms of automated surveillance technology include: the extent of information being gathered,[221] the context it is being gathered in,[222] and what type of information is being sought.[223]

### *B. Real-Time Search*

By comparison, real-time searches implicate Fourth Amendment protections to a greater extent than passive searches.[224] Real-time searches operate in real time, monitoring multiple people and conducting automated analysis instantaneously.[225] The privacy interests implicated are significantly greater than a passive search.[226] Where passive searches need input from humans, real-time search collects and gathers this information indiscriminately and infinitely.[227]

220. *See generally* Hirose, *supra* note 96 (discussing the implications of emergent surveillance technologies on Fourth Amendment protections.)

221. *See* Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018) ("detailed, encyclopedic, and effortlessly compiled.").

222. The context of the search has always played a role in the extent of protections granted under the Fourth Amendment. *See e.g.*, Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us about the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1404 (2010) (container searches); Bruce D. Hausknecht, *The Homicide Scene Exception to the Fourth Amendment Warrant Requirement: A Dead Issue*, 71 J. CRIM. L. & CRIMINOLOGY 289, 291 (1980) (emergency search); Lawrence T. King, *The Inventory Exception to the Fourth Amendment Warrant Requirement: Why the Last in Should be the First Out - Or, Putting Opperman and Bertine in Their Place*, 12 AM. J. TRIAL ADVOC. 273, 293 (1988) (inventory search); Kristina M. Woodworth, *The Significance of Oregon Constitutional Analysis in the Administrative Search Context after Action v. Vernonia School District 47J*, 75 OR. L. REV. 609, 609 (1996) (administrative search); Mark Goreczny, *Taking Care While Doing Right by the Fourth Amendment: A Pragmatic Approach to the Community Caretakers Exception*, 14 CARDOZO PUB. L. POL'Y & ETHICS J. 229 (2015) (home searches).

223. *See* Elle Xuemeng Wang, *Erecting a Privacy Wall against Technological Advancements: The Fourth Amendment in the Post-Carpenter Era*, 34 BERKELEY TECH. L.J. 1205, 1234 (2019) (article referring to certain types of information as "privacies of life" that deserve protection under the Fourth Amendment). *But see* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 556 (2016) (stating that distinguishing between types of information is not an effective method to protect Fourth Amendment privacy interests).

224. *See generally* Garvie & Moy, *supra* note 17. Real-time search is usually applied by leveraging sensors, which include cameras, across a wide network in the public to gather information about individuals on a continuous basis. Often, this process involves analyzing the characteristics of thousands of people moving in the public without any limitation on use. This type of search is some of the most intrusive, and it can often be very difficult to establish injury with this type of automated surveillance because not all use may result in criminal or civil charges, but rather contribute to an environment of distress and chilling of expression.

225. *Id.*

226. Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018) (the Court referred to cell site location data collected on the continuous basis as "detailed, encyclopedic, and effortlessly compiled."); Hirose, *supra* note 96 at 1608 ("the use of facial recognition clearly implicates privacy interests that are different from, and more than, the sum of its parts").

227. *See* Carpenter, 138 S. Ct. at 2209.

*Fourth Amendment Constraints*

The blanket use of real-time searches of any type is similar to developing a solution to find a needle in a haystack.[228] Through real-time searches, the information of millions of people will be gathered, and without limits, widespread constitutional breaches will occur.[229] Most importantly, the Fourth Amendment's particularity requirement (operating as a mechanism to establish probable cause prior to the commission of any crime or criminal activity) is almost automatically breached due to the nature of this technology. The scope of such a search operates in reverse of the particularity requirement.[230] Real-time searches collect vast amounts of data, and millions of people are analyzed to identify a single person. This flies in the face of the warrant requirement, which is that the government must conduct an investigation to establish probable cause, and then seek a warrant to either arrest a specific person or seize specific items.[231] Such an inversion presents serious Fourth Amendment concerns. The lack of probable cause mixed with the intrusive nature of the search undermines the privacy rights of the public.[232]

A warrant is the bare minimum requirement to conduct such a search.[233] Requiring temporally- and spatially limited searches of this type would be one of the fundamental safeguards to prevent overreach in real-time searches.[234]

### *C. Aggregation Problems*

The aggregation problem is a result of the mass collection of individual data.[235] Every time the data of an individual is probed for a possible match, it could

228. Harvey Gee, *Surveillance State: Fourth Amendment Law, Big Data Policing, and Facial Recognition Technology*, 21 BERKELEY J. AFR.-AM. L. & POL'Y 43, 80 (2021) ("[f]acial surveillance technology is . . . problematic because it casts such a wide net . . . indiscriminately search all faces").

229. Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post*-Carpenter, 26 BERKELEY J. CRIM. L. 71, 83 (2021).

230. Orin Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951, 952–57 (2009).

231. *See supra* Section III. Normally, particularity would require law enforcement to specifically describe the place or person being searched. Instead, automated surveillance involves the analysis of vast amount of data to identify a person and conduct additional analysis about them, without having to particularly describe the person or place.

232. *Id.*

233. *See* U.S. CONST. amend. IV.

234. *See* D. Gerber, *Types of Property Seizable under the Fourth Amendment*, 23 UCLA L. REV. 963, 964 (1976) ("[a] comprehensive school principal would provide that within certain spatial and temporal perimeter, the seizure of certain type of property is lawful"). *But see* Maryland v. Buie, 494 U.S. 325, 341–42 (1990) (Brennan, J., dissenting) (rejecting spatial and temporal restrictions as they are not effective in limiting the scope of searches).

235. Emily Berman, *When Database Queries are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579 (2017); Solove, *supra* note 48, at 511-16 (2006). Identification through aggregation essentially refers to a situation where to conduct analysis to identify one person their needs to be a dataset to cross-reference against millions of other people. This analysis can be flawed, biased, and incomplete, resulting in false positives, false negatives, and other types of injuries.

constitute a Fourth Amendment violation.[236] Nonetheless, it is not an injury that is easily remedied because its effect is dispersed and divided.[237] This results in difficulties in establishing standing to bring a claim.[238]

The aggregation problem leads to two unique issues. First, there is a risk of risk of incorrectly identifying an individual whose data has been aggregated with another individual, improperly triggering criminal processes.[239] Second, there could be potential dark zones in aggregated sources.[240] An example of a dark zone is a database collecting the images of people scraped from social media websites.[241] Any person who does not have any image on social media would be oblivious to any of these databases, even though they may have valid identification and other governmental documentation.[242] In such cases, overreliance on a database can cause incorrect determinations, which cannot be effectively remedied within the confines of the system.[243]

Failure to acknowledge these problems results in an increased likelihood of them occurring and reproduced in manners that may not be easily identified or remedied.[244]

### *D. Automation Process*

Many automated surveillance experts seek to automate complex analysis in the development of new surveillance systems.[245] The ability to provide law enforcement with rich, detailed information about particular individuals or things in the real world is poised to be a multibillion-dollar industry.[246] In particular, the

236. Berman, *supra* note 184, at 603.

237. Ferguson, *supra* note 61 at 1128 ("[large] scale surveillance systems have already created a difficult puzzle for standing determinations").

238. *Id.*

239. *See* Ferguson, *supra* note 61 at 1135 & 1198 (discussing the problems with aggregation and facial recognition data).

240. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 628 (2019).

241. *Id.*

242. Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253, 286 (2018).

243. *Id*.

244. *Id*.

245. Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 874-75 (2016).

246. Susan McCoy, *O'Big Brother Where Art Though: The Constitutional use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471, 473 n.8 (2002) (biometrics is expected to become a multibillion-dollar industry); *see* Mitra V. Yazdi, *The Digital Revolution and the Demise of Democracy*, 23 TUL. J. TECH. & INTELL. PROP. 61, 77 (2021).

provision of contextual information including movement, demographics, intent, and others, presents difficult questions regarding the scope of automated surveillance technology.[247]

Using automated surveillance technology to monitor individual behavior and report that behavior allows unprecedented access into an individual's autonomy in the public, including the right to move anonymously through the public.[248] In addition to the lack of cultural sensitivity, bias, and false positives, this technology goes beyond any reasonable notion of privacy whether in the context of modern technology or traditional constitutional law.[249]

Even in a passive manner, greater privacy interests are implicated compared to other forms of automated surveillance technology, through the extraction of contextual information.[250] While some of these inferences may be valid, they are based on the training of artificial intelligence models rather than the establishment of any probable cause necessary for the Fourth Amendment.[251]

## VI. PREVENTING AND REMEDIATING FOURTH AMENDMENT VIOLATIONS

This section offers recommendations for legislative and judicial bodies to mitigate the impact of automated surveillance technology and to safeguard the values enshrined in the Fourth Amendment. These recommendations are a synthesis of the analysis and research conducted in this paper, building upon the identified protections of the Fourth Amendment, and ameliorating the damage caused when automated surveillance technology is not used in accordance with the Fourth Amendment.[252]

These recommendations seek to supplement existing protections available to individuals for Fourth Amendment violations, including: the application of the

247. Fortune Business Insights, *Biometric System Market Size Worth USD 76.70 Billion by 2029* (Jan 17, 2023), https://www.globenewswire.com/news-release/2023/01/17/2589810/0/en/Biometric-System-Market-Size-Worth-USD-76-70-Billion-by-2029-Report-by-Fortune-Business-Insights.html ("the market is categorized into face recognition, iris recognition, voice recognition, vein recognition, fingerprint recognition, and others").

248. Rich, *supra* note 246, at 873-74.

249. *See* John Zens, *Face It: Only Congress Can Preserve Privacy from the Pervasive Use of Facial Recognition Technology by Police*, 58 SAN DIEGO L. REV. 143, 153–54 (2021).

250. *Id.* at 154.

251. Benedict, *supra* note 86, at 867-68 (discussing the difficulty in establishing probable cause based on facial recognition technology).

252. *See infra* Section VII.A-G.

exclusionary rule[253] and *Bivens* actions, which have developed in response to evolving requirements.[254]

### *A. Expungement*

One of the most devastating impacts of an arrest, whether pursuant to the use of automated surveillance technology or not, is the secondary effects on an individual.[255] Often individuals are arrested at their homes or places of work, straining the relationships with others.[256] It places doubt on a person's character. In addition, the jail-to-prison pipeline is designed to gather as much information about an individual as possible without any regard for the impact this will have on their life.[257] A person is forever marked as having been arrested, their personal identifiers seized, and their information subject to analysis in future searches for possible matches.[258] Once this information has been collected, it is generally available to the public when conducting background searches and analyses.[259]

One of the potential remedies to ensure the preservation of Fourth Amendment protection, especially when someone has been subject to an unlawful search conducted without probable cause, is to expunge all of the information collected about a particular individual.[260] While an individual can petition the court to

253. Mapp v. Ohio, 367 U.S. 643, 655 (1961) (establishing the exclusionary rule).

254. Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 397–98 (1971) (establishing *Bivens* action giving an implied right of action to recover "money damages for any injuries he has suffered as a result of the agents' violation of the [Fourth] Amendment.").

255. Kathryn Zickuhr, *Applying a Racial Equity Lens to Fines and Fees in the District of Columbia*, DC POLICY CENTER (Apr 22, 2019), https://www.dcpolicycenter.org/publications/racial-equity-fines-fees/ (discussing secondary effects such as "job loss or eviction"). *See* Wayne A. Logan, *Government Retention and Use of Unlawfully Secured DNA Evidence*, 48 TEX. TECH L. REV. 269, 280–81 (2015) (explaining the difficulty of getting an criminal expungement).

256. Robyn E. Metcalfe et al., *Witnessing Parental Arrest As a Predictor of Child Internalizing and Externalizing Symptoms during and after Parental Incarceration*, J. CHILD & ADOLESCENT TRAUMA 1, 2 (2022); Eric Martin,

*Hidden Consequences: The Impact of Incarceration on Dependent Children*, NAT. INST. JUSTICE, DEP'T OF JUSTICE (Mar 1, 2017), https://www.ojp.gov/pdffiles1/nij/250349.pdf ("children whose parents are incarcerated are at higher risk for increased antisocial behaviors").

257. Lawrence J. Leigh, *Informational Privacy: Constitutional Challenges to the Collection and Dissemination of Personal Information by Government Agencies*, 3 HASTINGS. CONST. L.Q. 229, 235 n.8 (1976) ("unfettered dissemination of such damaging and potentially misleading information as raw arrest records is permitted, it will be extremely difficult to sustain any constitutional challenge to the collection and use of personal information").

258. *Id.*

259. Sarah E. Lageson, *Digitizing and Disclosing Personal Data: The Proliferation of State Criminal Records on the Internet*, 46 L. & SOC. INQUIRY 635, 661-62 (2021).

260. Surell Brady, *Arrests without Prosecution and the Fourth Amendment*, 59 MD. L. REV. 1, 63 (2000) (advocating for expungement as criminal records may follow individuals even if they have been acquitted). *See*

expunge their record, not many people have the contextual knowledge of the legal system to effectively navigate these problems without facing roadblocks in continuing their employment, education, and social relations.[261]

The ideal solution would be to have an automatic process by which a person's arrest record is expunged when they are arrested based on automated surveillance technology that may have resulted in a false-positive.[262] In addition to process-based expungement protections, ethical obligations can be placed on judges and prosecutors to ensure that a person's innocence is restored retroactively, minimizing the cost to the individual subject to an unlawful search.

### *B. Recalling Warrant*

A warrant issued based on faulty automated surveillance technology can subject an individual to police searches, with a presumption that probable cause had already been established.[263] Often when a person is arrested, many of their outstanding warrants remain on the record, subjecting them to future searches and seizure even though in a particular instance no formal charges were brought.[264]

The use of automated surveillance technology creates a dangerous situation where misidentification of identity or behavior can result in potential criminal sanctions despite a lack of guilt. In such situations, the necessity for judicial oversight is greater than ever, and can be met with providing an independent arbiter to review the available material on a case-by-case basis to ensure that it complies with the requirements of the Fourth Amendment.[265] Otherwise, law enforcement could simply conduct an arrest pursuant to an outstanding arrest warrant in subsequent instances, allowing for harassment by law enforcement.[266] A warrant needs to be specifically reviewed when requested based on research

*generally* Elizabeth E. Joh, *Myth of Arrestee DNA Expungement*, 164 U. PA. L. REV. ONLINE 51, 59 (2015-2016) (proposing automatic expungement for DNA data collected in violation of the law).

261. Brady, *supra* note 259 at 63.

262. *See* Joh, *supra* note 259 at 59.

263. Bah v. Apple Inc., No. 19-CV-3539 (PKC), 2021 WL 4084500, at *8-10 (S.D.N.Y. Sept. 8, 2021) (discussing the question of whether facial recognition can be used establish probable cause); Benedict, *supra* note 86, at 895 n.343 (2022) (discussing why facial recognition should not be the sole basis to establish probable cause).

264. Michael Kimberly, *Discovering Arrest Warrants: Intervening Police Conduct and Foreseeability*, 118 YALE L. J. 177, 179 (2008) (discussing that an open warrant may fail to prevent future unconstitutional detentions); Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L. J. 2054, 2141 (2017) (evidence that was otherwise inadmissible because of the Fourth Amendment was admitted because of an open warrant).

265. *See* David A. Moran, *Hanging on by a Thread: The Exclusionary Rule (Or What's Left of It) Lives for Another Day*, 9 OHIO ST. J. CRIM. L. 363, 369–70 (2011) (discussing how the Supreme Court continues to reiterate what the purpose of the exclusionary rule is – to deter police violations of the Fourth Amendment).

266. *Id*. at 364 (explaining how law officers have access to a police database for outstanding arrest warrants to justify potential searches).

conducted using automated surveillance technology. This would require a judicial actor to review the information in light of its technological limitations and the potential dangers it poses for individuals.

### *C. Notice of Identification*

The notice of identification operates at two levels.[267] First, during the stage of requesting a warrant, the proceeding takes place on an *ex parte* basis without representation of the potential arrestee.[268] In such a case, notice that probable cause has been established in part because of the usage of automated surveillance technology can help judges make more informed decisions about whether the application meets the requirements for particularity established by the Fourth Amendment.[269]

Second, once law enforcement arrests an individual or seizes their things, the availability of information on the record indicating that the warrant was obtained through the use of automated surveillance technology can play a significant role in challenging criminal charges.[270] In the most extreme cases, an individual would simply need to show that any identification made by the system was incorrect, and as a result, the charges and warrant lack any form of merit.[271] However, there are situations where an individual may also be able to raise questions as to the validity of the warrant, any action in pursuance of the warrant, and the analysis provided by the system.[272] This can include questions of whether the warrant was particular enough, or whether probable cause was established based on the use of automated surveillance technology.

267. *See generally* Harry Aniulis, *Facial Recognition Technology, Privacy and Administrative Law*, 45 U.N.S.W.L.J. 1513, 1516 (2022) (noting the lack of consent in ascertaining identity using facial recognition); David Gray, *Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies*, 24 SMU SCI. & TECH. L. REV. 3, 51 (2021) (observing the lack of notice and consent of individuals whose data is included within facial recognition databases). The two criteria identified are: the *ex parte* basis on which a warrant is granted and explicitly noting the use of automated surveillance in procuring the warrant.

268. Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders*, 93 WASH. L. REV. 145, 168 (2018) ("proceedings for the issuance of the orders are historically ex parte") (discussing the ex parte nature of warrants and surveillance orders with reference to the First Amendment).

269. Ferguson, *supra* note 61, at 1203.

270. *See generally* Garvie & Moy, *supra* note 17.

271. Automated surveillance can frequently produce incorrect results (*see supra* Section VI). By incorporating this information into a warrant provides an individual subject to a search the opportunity to challenge the results of the automated surveillance. This can serve as an important safeguard to ensure that there actually is probable cause and particularity based upon which a word was granted. If the information is soon to be incorrect, then the warrant can be invalidated and any evidence procured through the warrant should be rendered inadmissible.

272. *See generally* Garvie & Moy, *supra* note 17 (explaining that while there are public safety benefits to the surveillance system, there are concerns for biometric privacy and other Constitutional rights).

Having available information that identification or other forms of evidence were collected from automated surveillance technology would facilitate transparency in the criminal process needed to challenge state action.

### *D. Independent Supervision of Surveillance Methodology*

One of the main recommendations provided by the GAO to other federal agencies, including the FBI and Department of Justice (DOJ), is the need for greater independent scrutiny of the usage of facial recognition.[273] A major problem with facial recognition technology is the risk of high false-positive rates, which in turn directly affect the reliability of any results produced from the system.[274] Further, the technology may incorrectly identify other behavioral traits that may be the basis for inferences drawn with regard to evidence.[275]

To address these problems, it should be mandatory for agencies to monitor the efficacy of the technology and conduct a privacy impact assessment. The goal of efficacy monitoring is to ensure that if there is a risk of incorrect identification, it is immediately documented, and remedial actions are taken to ensure that any identification made is accurate.[276] Public documentation of the rates of inconsistency provides individuals with a fair opportunity to challenge facial recognition determinations, in addition to creating consistency in expectations.[277]

In addition to efficacy monitoring, conducting privacy impact assessments provides an opportunity to understand the application of the technology by a particular agency as an aggregate.[278] Generally, the public is made aware of the usage of automated surveillance technology through the reporting of extreme aberrations,[279] like those of Robert Williams.[280] However, privacy impact assessments change this dynamic by providing insight into the intent and goals of an agency in the application of automated surveillance technology, including comprehensive statistics of its usage during previous years.[281] This can allow

273. U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 18-19 (May 2016).

274. *See generally* PATRICK GROTHER ET AL., NAT'L INSTITUTE OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2 (2019) (describing how people of color, women, and old and young individuals have disproportionately high facial recognition false positive rates).

275. *See supra* Section III.B.

276. *See generally, e.g.*, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES (2020) (illustrating efficacy monitoring of ICE's facial recognition program).

277. Ferguson, *supra* note 61, at 1207 (discussing auditing of facial recognition technology as a precondition for use, revealing error rates, accuracy, and providing a method for accountability).

278. Accountability, *supra* note 137, at 26.

279. *Id.* at 25.

280. Hill, *supra* note 1.

281. Accountability, *supra* note 180, at 17–18 (listing how the FBI and six other federal agencies used a photo database to support criminal investigations).

policymakers and media to comprehensively offer the public recommendations to limit the technology in a manner consistent with the Fourth Amendment, ensuring democratic oversight over this technology. The failure to include reports can be grounds to limit funding, conduct investigations into the usage of automated surveillance technology, and limit future surveillance activities.

### *E. Additional Limits on "General Warrant"-Like Surveillance*

This recommendation targets real-time surveillance methods due to the extent and impact this type of technology has on the public and individuals.[282] Real-time surveillance creates a panopticon type surveillance in the real world, offering virtually no protection from prying eyes.[283] The state can use this information with little to no oversight to harass individuals and curb freedoms without relying on democratic processes.[284] The extent of such information can allow the government to track individuals, identify intent, and curb any form of dissent.[285]

The enormous interests implicated with the usage of real-time surveillance require similar protections to prevent proportionately enormous governmental overreach.[286] The reach of such type of real-time surveillance can be likened to the "general warrants" [287] that the Founders had raised concerns about when enacting the Fourth Amendment. Arguably, real-time surveillance goes far beyond those reaches, since a general warrant would still be limited by the physical capabilities of law enforcement.[288] Automated surveillance technology is subject to virtually none of the limits of a human, requiring no sleep or rest, no payment for sustenance, and subject to no physical limits.[289] The use of real-time surveillance necessarily needs to be supported by a warrant and probable cause. The particularity requirement, which requires the place to be specifically identified and the person or things to be seized to be particularly identified, will serve as the

282. *See generally* Hirose, *supra* note 96.

283. *Id.* at 1591.

284. Steven I. Friedland, *Transmogrifying Privacy: The Impact of the Internet of Things on Open Government*, 7 INT'L J. OPEN GOV. 1, 9 (2018) ("accumulation of data without a specific purpose equates to the general warrant of old"); Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age after Carpenter?*, 26 B.U. J. SCI. & TECH. L. 286, 295 (2020) (comparing the third-party doctrine to general warrants).

285. *See generally* Hirose, *supra* note 96 at 1618–19 (discussing how facial recognition could be used to monitor protests, travel, and medical conditions).

286. *See generally* Friedland, *supra* note 285.

287. *See* Entick v. Carrington (1765) 95 Eng. Rep. 807, 810 (KB) (illustrating a general warrant in colonial England).

288. Bonnie E. Devany, *Clearview AI's First Amendment: A Dangerous Reality?*, 101 TEX. L. REV. 473, 481 (2022) (discussing how real-time surveillance can encroach on the freedoms of people by constantly watching them and limiting their ability to move freely in the public).

289. *See* Zalnieriute, *supra* note 169, at 292-93 (2021) (contrasting the significance of automated facial recognition with other, non-automatic surveillance such as fingerprints).

primary limit on overreach using real-time surveillance amounting to "general warrant" like search.[290] The judiciary should require executive agencies requesting the usage of real-time surveillance to show that no other reasonable method with sufficient particularity can be established in order to conduct the search or seizure being requested. Once the person has been arrested, or thing has been seized, law enforcement should have a responsibility to delete any information gathered by the real-time surveillance of bystanders to prevent government overreach.[291]

In such situations it is also necessary to limit the applicability of exceptions to the Fourth Amendment.[292] First, the community caretaking exception could potentially spell severe consequences for undercutting liberties where law enforcement could argue that under its power for "community caretaking", it can infringe into the lives of individuals.[293] The exact contours of this exception are imprecise, operating whenever law enforcement is not interacting with individuals in pursuance of a criminal act yet uncover potentially incriminating information.[294] Even though this exception has been circumscribed, its revival spells major concerns with reference to general warrants.[295] Second, the third-party doctrine needs to be reformed to specify what type of records a person provides with consent are subject to lowered expectations of privacy.[296] The judiciary needs to clarify if the data has been collected without a person's permission or informed consent, and whether it would be subject to the third-party doctrine, since they did not consent to the disclosure of their information, even if that information was available within a certain segment of the public.[297] Finally, the good faith exception[298] should be limited to take into account requirements to provide notice and reasonable opportunity to challenge incorrect or improper usage of automated surveillance technology.

290. *See* Brandon V. Stracener, *It Wasn't Me – Unintended Targets of Arrest Warrants*, 105 CALIF. L. REV. 229, 234-35 (2017) (describing Supreme Court caselaw regarding the particularity requirement for warrants).

291. *See, e.g.*, Accountability, *supra* note 180, at 49 (describing how Customs and Border Protection deletes facial recognition images within 12 hours after a match).

292. *See* Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) (describing the high legal standard required to establish an exception under the Fourth Amendment).

293. *See* Privacy and Surveillance Accountability, *supra* note 127, at 3 (warning that extending the community caretaking exception to the home could lead to future intrusions into electronic devices).

294. *See supra* Section I.D.2.

295. *See* Friedland, *supra* note 285 at 9.

296. *See* Rozenshtein, *supra* note 117, at 946, 950 (quoting academics claiming the third-party doctrine became extinct after *Carpenter v. United States*, whereas lower courts still apply the doctrine).

297. *Id*.

298. *See generally* Harrison, *supra* note 129 (describing the seminal Supreme Court cases outlining the good faith exception).

### *F. Particularity and the Person*

While a person's movement in public, demographic information, and identity can reasonably be regarded as "things" under the Fourth Amendment, the judiciary should consider expanding on the jurisprudence involving "particularly describing . . . persons . . . to be seized."[299] Most cases have not focused on this aspect of the Fourth Amendment, likely because particularly describing an individual has never been a major concern when conducting Fourth Amendment limited actions.[300] When law enforcement normally requests a warrant, they have identified the individual.[301] In situations where a person has not been identified, a warrant is should be accompanied by identifiers.[302] Another situation where a person's identity may be implicated is when they are asked to produce their identification to law enforcement.[303] In most cases, the judiciary has upheld such requirements.[304] Simply relying on a person's identity as determined through the use of automated surveillance technology can have severe consequences, and undermines of democratic freedoms that go beyond the scope of the Fourth Amendment.[305]

By defining the scope of particularity and the person, the judiciary can provide guidance on the scope of interests protected by the Fourth Amendment when a person is subject to automated surveillance technology.[306]

### *G. Remedies for Aggregation Problems*

Where an individual has been incorrectly identified by automated surveillance technology and has not been provided a reasonable opportunity to challenge such

299. U.S. CONST. amend. IV.

300. Daniel L. Rotenberg & Lois B. Tanzer, *Searching for the Person to be Seized*, 35 OHIO ST. L.J. 56, 56-58 (1974) (describing the distinction between arrest and search warrants, noting that a search warrant does not require "prior judicial finding of the need for the police to search or of the probability that the search will be fruitful").

301. *See id*.

302. Ryan Webb, *What's in a Name: A Case for Including Biometric Identifiers on Arrest Warrants*, 47 LOY. L. A. L. REV. 319, 321-23 (2013) (using biometrics to distinguish between people because people may have similar identifying characteristics).

303. James G. Warner, *Dudley Do Wrong: An Analysis of a Stop and Identify Statute in* Hiibel v. Sixth Judicial District Court of Nevada, 39 AKRON L. REV. 245, 262 (2006) (even though people have a privacy interest in their identity, it has traditionally never been included within Fourth Amendment protections); Hiibel v. Sixth Jud. Ct. of Nev., 542 U.S. 177, 177-84 (2004) (producing identity does not receive protection under the Fourth Amendment).

304. People v. Mitchell, 678 P.2d 990, 993 (Colo. 1984) (discussing particularity with reference to the person).

305. *See* Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1514 (2022) (discussing the effect broad government surveillance has on democratic freedoms and human rights).

306. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 439 (1974) (an independent judiciary plays an important role in regulating the Fourth Amendment).

identification, there may be a need for further remediation beyond those discussed above.[307] If they were merely accused as a result of their data being aggregated into an enormous database containing the data of millions of other people, resulting in a false-positive this may be the result of data aggregation. The dangers of aggregation are apparent and severe for the public in general, particularly for individuals subject to criminal processes as a result of the failure of such technology.[308] Any legal cost, lost wages, loss of reputation in the community, and emotional damage should be remedied through monetary compensation and an injunction against future warrants or charges on the same or similar charges.[309]

The goal of such remedies is to limit executive discretion and ensure that the system affords people protection against government intrusion.[310] It is also designed to ensure that any determination ultimately made by surveillance technology is reviewed by a human for accuracy.[311] These remedies are a safeguard to protect against deviation from due process and a deterrent for the State to guard against unscrupulous actions.

## CONCLUSION

As companies providing automated surveillance solutions have secured their position as indispensable tools, citing the benefits they provide in curbing criminal activities and terrorism, there is an urgent need on behalf of legislative and judicial bodies to act on these growing trends. While there is an undoubted interest that is being safeguarded through such surveillance, the Constitution has given primacy to the liberties vested in people to be safe in their homes and that their private affairs are not subject to arbitrary examination by the state. The state can only infringe on the constitutional right to privacy as protected by the Fourth Amendment when certain criteria have been met, namely, a warrant, supported by probable cause, which is particularly defined. The need for independent review by the judiciary serves as a barrier against the impulsive tendencies of law enforcement.

This article establishes that the usage of automated surveillance technology and facial recognition is subject to the protections of the Fourth Amendment. Automated surveillance technology includes all forms of surveillance that monitors people and things with little to no human oversight. Throughout the country,

307. *See* Berman, *supra* note 184, at 584 (arguing that certain data queries using aggregated data sets should be considered Fourth Amendment searches).

308. *See supra* Section V.C.

309. *See supra* Section V.C.

310. *See supra* Section I.A.

311. Sarah Chun, *Facial Recognition Technology: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility*, 21 N.C. J.L. & TECH. 99, 112 (2020) (the need for human review of facial recognition technology to prevent violations of human rights through the use of the technology).

government agencies are adopting automated surveillance technology like facial recognition software. These can be a mix of public and private solutions developed specifically for the purpose of monitoring public activity. There are at least twenty federal agencies using facial recognition technology and over 2,000 police departments throughout the country at both the state and municipality level. In the vast majority of cases, this technology is operating with no oversight barring internal guidelines and review mechanisms adopted by these law enforcement agencies for the purpose of regulating its use.

The pressing nature of this concern exacerbates the need for criminal procedural protections limiting executive discretion and protecting privacy interests that are a risk of being disregarded by government agencies. Accordingly, this article provides an in-depth discussion of why the Fourth Amendment particularity requirement is applicable to automated surveillance technology and facial recognition.

This article begins this analysis by exploring the theoretical foundations of the Fourth Amendment and their relationship with automated surveillance technology. First, there is a need to limit executive discretion and decision-making when applying this technology, because of the significant privacy interests its use implicates. Currently, the lack of oversight is startling and allows executive agencies to operate with impunity with regard to the growing proliferation of technology such as facial recognition solutions. Second, a strong privacy interest is involved with the use of facial recognition and other automated surveillance technology. While an individual generally may not receive the protections of the Fourth Amendment for an officer merely observing their movements, the protections would be applicable with reference to automated surveillance technology because of the type of information that is available to law enforcement through this technology. It can immediately and seamlessly access databases containing millions of records identifying individuals, and further gather information about a person's movements, demographics, and behavioral characteristics.

A reasonable expectation of privacy can also be established by highlighting the fact that the information disclosed by such technology cannot be identified by law enforcement without the use of the technology, the individual seeks to keep most of this information private, and the policy interests protecting individuals outweigh the government's interest.

The overwhelming individual interest protected by the Fourth Amendment is subjected to some limited exceptions such as the third-party doctrine, community caretaking doctrine, and good faith exception to the warrant requirement. Although courts have consistently held that the exceptions to the Fourth Amendment should be narrowly construed, they are nonetheless important in understanding its applicability and the potential grey areas where the Fourth Amendment would be unable to protect individuals from government oversight.

The particularity requirement itself has only a few requirements, including the requirement to specifically define the person or things being seized or searched,

limit executive discretion, define the space to be searched, and ensure that the warrant operates for a limited time. Because of its nature, it is a fact intensive inquiry.

This article concludes with the acknowledgment that the usage of automated surveillance technology and facial recognition presents grave concerns to individual liberty and autonomy with reference to the Fourth Amendment. To address the potentially significant consequences resulting from the application of these types of technology, this article proposes a series of recommendations that can be adopted by policymakers and the judiciary in order to better safeguard the interests of people in a highly interconnected world. Recognizing this reality, some of the potential remedies to protect against government overreach include the immediate and automatic expungement of arrest warrants, arrest records, and criminal charges associated with the usage of automated surveillance technology once an individual is adjudicated to be innocent or no charges are brought against them. The second remedy involves recalling outstanding warrants, which can establish probable cause for a crime where the police may not have established a sufficient nexus. This seeks to limit executive discretion in the real world, where an individual could be arrested based on such records for wholly unrelated activities.

The third requires law enforcement to provide the judiciary with notice that the evidence they have gathered to establish probable cause for a warrant is based on the usage of automated surveillance technology or facial recognition. The notice will also provide an individual the opportunity to subsequently challenge the information collected by law enforcement, where it has raised a false-positive, incorrect behavioral identification, or some other form of aggregation-related problem. The fourth involves independent supervision of the usage of automated surveillance technology. This requires regular auditing and publishing privacy impact assessments of automated surveillance technology to ensure it remains efficacious and accurate, and if there is any risk of bias or false positives in certain circumstances, it must be identified and disclosed to the public to mitigate bad faith actions.

The fifth provides for limits on the usage of facial recognition where no exception to the Fourth Amendment applies. This particularly applies to the usage of real-time automated surveillance and facial recognition, which have the potential to implicate multiple constitutional interests through their use. In reality, the usage of such technology is similar to rummaging through a person's personal belongings. By limiting the usage of this technology, courts can play an active role when such warrants are to be granted. The sixth is in the application of the particularity requirement of the person. While a person's personal information such as their demographics, movement, and identity, can reasonably be regarded as "things", the person themselves is also subject to the particularity requirement. The judiciary should elaborate on the application of particularity to the person, so as to prospectively limit the dangers associated with automated surveillance technology.

The final applies to individuals who are falsely accused as a result of automated surveillance technology or facial recognition technology. Where there was insufficient oversight in identifying a particular person, they should be afforded additional remedies in terms of monetary compensation and an injunction protecting them from further prosecution. The monetary compensation, in particular, should address economic losses resulting from lost wages, legal fees, reputational harm, and emotional injury, raising the stakes for the State in the event of misuse of the technology.

Policymakers and the judiciary can ensure the protection of the Fourth Amendment in a world teeming with emerging technology. Expanding jurisprudence on privacy interests protected by the Fourth Amendment and requiring law enforcement to show particularity when using this far-reaching technology would be one of the first steps in ensuring that the interests of the individual are protected while the public benefits from this technology.