Idaho Law Review

Volume 55 | Number 3 Article 5

The Perfect Storm: How Narrowing of the State Action Doctrine, Inconsistency in Fourth Amendment Caselaw, and Advancing Security Technologies Converge to Erode Our Privacy Rights

Matthew M. Meacham

THE PERFECT STORM: HOW NARROWING OF THE STATE ACTION DOCTRINE, INCONSISTENCY IN FOURTH AMENDMENT CASELAW, AND ADVANCING SECURITY TECHNOLOGIES CONVERGE TO ERODE OUR PRIVACY RIGHTS

MATTHEW M. MEACHAM

FULL CITATION:

Matthew M. Meacham, *The Perfect Storm: How Narrowing of the State Action Doctrine, Inconsistency in Fourth Amendment Caselaw, and Advancing Security Technologies Converge to Erode Our Privacy Rights*, 55 IDAHO L. REV. 309 (2019).

THE PERFECT STORM: HOW NARROWING OF THE STATE ACTION DOCTRINE, INCONSISTENCY IN FOURTH AMENDMENT CASELAW, AND ADVANCING SECURITY TECHNOLOGIES CONVERGE TO ERODE OUR PRIVACY RIGHTS

MATTHEW M. MEACHAM*

ABSTRACT

Security technology is advancing at a remarkable rate. While advances in security technology have the potential to help prevent gun violence and terrorism, the same technology is also capable of intruding upon our personal freedom and personal right to privacy. Development of the "Patscan" marks the beginning of new generation of weapons detection security technology. It is far more sophisticated than any weapons detection technology to date and gives rise to significant constitutional concerns. Current Supreme Court jurisprudence has yet to address the Fourth Amendment concerns inherent within the government's use of advancing security technology to search citizens of the United States. A narrow state action doctrine complicates the issue by undermining the Fourth Amendment's privacy protections. This note is intended to fill the gap in the Fourth Amendment conversation created by the emergence of the Patscan, while also illustrating the consequences of applying the exceptions to the state action requirement narrowly.

TABLE OF CONTENTS

---

* Member of *Idaho Law Review*, J.D. candidate, University of Idaho College of Law, 2019. I thank Professor Kristina Running for her guidance throughout the writing process, helpful feedback, and valued mentorship. Any errors are mine.

I. INTRODUCTION

> *"New technologies test the judicial conscience. On the one hand, they hold out the promise of more effective law enforcement, and the hope that we will be delivered from the scourge of crime. On the other hand, they often achieve these ends by intruding, in ways never before imaginable, into the realms protected by the Fourth Amendment"*[1]

When the Fourth Amendment was drafted and adopted, searches were physical acts carried out by a government agent rummaging through an individual's belongings, entering an individual's property, or requiring the individual to reveal objects carried on his person.[2] At the time the Fourth Amendment was adopted, law enforcement would have had to physically stop an individual and demand to see the contents of his pockets or bag to detect contraband carried on his person. But today the ability to search an individual using advanced technology without any physical invasion is becoming more and more of a reality. A variety of security technologies are available, or will soon be available, to both government and private security forces and law enforcement officers. The familiar metal detector allows security personnel at checkpoints, such as in airports, to search individuals for metal objects in hopes of preventing weapons from entering sensitive areas.[3] Handheld

1. United States v. Kincade, 379 F.3d 813, 871 (9th Cir. 2004) (Kozinski, J., dissenting).

2. *See generally* United States v. Jones, 565 U.S. 400, 406 (2012) ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' (internal citation omitted) As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government *trespass* upon the areas ('persons, houses, papers, and effects') it enumerates." (emphasis added)).

3. Michael Bernzweig, *Understanding and Selecting Walk Through Security Metal Detectors*, METALDETECTOR.COM, https://www.metaldetector.com/learn/buying-guide-articles/security-use/understanding-selecting-walk-through-security-metal-detectors (last visited Mar. 24, 2019).

concealed object detection systems are available for police forces to utilize while on patrol.[4] Security robots equipped with thermal imaging may detect suspicious heat signatures given off by a person's body,[5] which could be a weapon carried on their person. Even security patrol drones can now be equipped with thermal imaging and microwave sensor technology, allowing them to follow and scan any individual within their patrol range.[6] Technology allows for a search that is far more sophisticated than the physical inspection of an individual's belongings envisioned by the drafters of the Fourth Amendment. Because Fourth Amendment caselaw has been slow to grapple with the constitutional implications of these modern technologies and devices, legal scholars have often stepped in to fill the gap.[7]

The Patscan, developed by PatriotOne Technologies (PatriotOne), is an emerging weapons detection technology that makes the previously discussed technologies seem as crude and unsophisticated as the physical searches they were intended to replace.[8] The Patscan is a device that does far more than indicate whether an individual might be carrying a weapon.[9] It positively identifies whether an individual is carrying a concealed weapon, describes what type of concealed weapon the individual is carrying with a startling degree of specificity, and sends the information to all on-duty security personnel via mobile application, SMS, or computer interface.[10] The Patscan has the potential to revolutionize the appearance, perception, and efficacy of security checkpoints in a diverse set of applications. However, just like the technologies before it, the Patscan will challenge our understanding of the Fourth Amendment, creating yet another gap in Fourth Amendment caselaw.

---

4. *Thermal Vision Concealed Object Detection*, THERMAL MATRIX USA, http://www.thermalmatrixusa.net/# (last visited Mar. 24, 2019). These concealed object detection systems can be used to detect a variety of threats to both the public and law enforcement officers, including explosives, firearms, flammable liquids, and knives. *Id.* The concept of a handheld weapons detection system or "gun detector" dates back to the mid-1990s. *See* David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1 (1996). For an in-depth discussion of the Fourth Amendment implications of handheld gun detection technology see *id. See also* Sean K. Driscoll, *"The Lady of the House" vs. A Man with a Gun: Applying Kyllo to Gun-Scanning Technology*, 62 CATH. U.L. REV. 601 (2013).

5. *See* KNIGHTSCOPE, https://knightscope.com (last visited Mar. 24, 2019).

6. *Aerial Protection Service*, APTONOMY, http://www.aptonomy.com/ (last visited Mar. 24, 2019).

7. *See, e.g.*, Driscoll, *supra* note 4 (filling the Fourth Amendment gap regarding handheld "gun detectors"); Michael Ferraraccio, *Metal Detectors in the Public Schools: Fourth Amendment Concerns*, 28 J. L. & EDUC. 209 (1999) (filling the Fourth Amendment gap regarding the use of metal detectors in schools); Gregory S. McNeal, *Drones and the Future of Aerial Surveillance*, 84 GEO. WASH. L. REV. 354 (2016) (filling the Fourth Amendment gap regarding police use of drones to conduct surveillance).

8. *See Patscan CMR Data Sheet: Covert Weapons Detection System*, PATRIOTONE TECH., http://sengex.com/wp-content/uploads/2017/10/Patriot1-Spec-Sheet.pdf (last visited Mar. 24, 2019) [hereinafter PatriotOne, *Data Sheet*].

9. *Id.*

10. *See Overview: Patscan Product Demonstration Video*, PATRIOTONE TECHNOLOGIES, https://patriot1tech.com/solutions/overview/ (last visited Mar. 24, 2019) [hereinafter PatriotOne, *Product Demonstration Video*].

This note is intended to grapple with the constitutional concerns raised by the development of the Patscan and to fill the gap in Fourth Amendment caselaw and literature that the Patscan creates. Part II of this note will provide background information on the Patscan itself by briefly describing its features and capabilities, as well as comparing and contrasting the Patscan to current checkpoint security technology, such as metal detectors and millimeter wave scanners.[11] Part III provides relevant background information on the current state of the state action doctrine and Fourth Amendment jurisprudence.[12] Part IV will then apply the state action doctrine and current Fourth Amendment caselaw to the use of the Patscan device in a number of common contexts, such as in airports, government buildings, high schools, and sports stadiums, to evaluate the constitutionality of its use in those contexts.[13] Finally, Part V will conclude and briefly discuss the need for judicial re-evaluation of the trend favoring security over privacy when it comes to emerging technologies and the Fourth Amendment, as well as the important role the state action doctrine should play in protecting privacy in the 21st century.[14]

II. BACKGROUND ON THE PATSCAN

According to PatriotOne, "P[atscan] CMR is the world's most advanced technology for covert screening and detection of concealed weapons."[15] PatriotOne also claims that it developed the Patscan "as an effective tool to combat active shooter threats before they occur . . . thereby diminishing the epidemic phenomena of active shooters across the nation."[16]

A. What Makes the Patscan Unique?

The Patscan uses cognitive microwave radar technology to detect and identify weapons.[17] Cognitive microwave radar works through the emission of microwaves in the direction to be searched.[18] These waves bounce off the human body at a different level than they do when being reflected off of concealed objects, allowing the device to determine whether someone is carrying an object.[19] Once the different frequencies are received by the Patscan device, "sophisticated software algorithms analyze the data to identify any concealed objects."[20] The system then compares the signal to a database of pre-loaded weapon patterns and, if the weapon pattern is already present in its database, identifies the weapon to a high degree of specificity.[21] The device not only positively identifies the weapon, but it also

11. *See infra* Part II.
12. *See infra* Part III.
13. *See infra* Part IV.
14. *See infra* Part V.
15. PatriotOne, *Data Sheet*, *supra* note 8.
16. *Id.*
17. *See Patscan CMR: Cognitive Microwave Radar*, PATRIOTONE TECHNOLOGIES, https://patriot1tech.com/solutions/patscan-cmr/ (last visited Mar. 24, 2019) [hereinafter PatriotOne, *Patscan CMR*].
18. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10.
19. *See* PatriotOne, *Patscan CMR*, *supra* note 17.
20. *See id.*
21. *See id.*

provides detailed information about the weapon when available.[22] For example, if a gun is detected that matches one of the profiles stored in the Patscan's database, it can provide information such as the caliber of the firearm, the capacity of the magazine, the barrel length, action type, grip size, and the type of metal the gun is machined from.[23]

The "cognitive" part of the process is that the device "learns" over time by adding unidentified weapon patterns to its database as it encounters them.[24] Then, the device will share the new weapon pattern data across the system's network so that all Patscan devices will be capable of detecting the new weapon type.[25] The Patscan has an effective range of about two meters, making it most useful in entry-ways and high foot-traffic areas.[26]

B. Patscan vs. Metal Detectors vs. Millimeter Wave Scanners

Because the Patscan is most likely to be used in applications similar to metal detectors and millimeter wave scanners, its features are best described when viewed in comparison to those security technologies. The Patscan is similar to metal detectors and millimeter wave scanners in the fact that all three devices are used to screen individuals with the goal of detecting weapons.[27] Similarities between the Patscan and other stationary weapons detections systems end there, however.

Metal detectors are very effective at doing what they are designed to do, detect metal.[28] Metal detectors indiscriminately detect any metal object that disrupts the magnetic field produced by the device as an individual passes through the scanner.[29] Objects such as gum wrappers, pens, key rings, metal eye glasses, and

22. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10.

23. *See id.*

24. *See* PatriotOne, *Patscan CMR*, *supra* note 17.

25. *See id.*

26. PatriotOne, *Data Sheet*, *supra* note 8.

27. Metal detectors are likely one of the first security devices that come to mind for many when thinking about security checkpoints in airports and certain secure government facilities. Metal detectors are commonplace security devices with a primary purpose of detecting metal objects that could be used as weapons including knives, guns, and certain explosives. *See* Bernzweig, *supra* note 3. Millimeter wave scanners are full-body scanners that search for concealed weapons or devices using radio waves. *See* Markham Heid, *You Asked: Are Airport Body Scanners Safe?*, TIME (Aug. 23, 2017), http://time.com/4909615/airport-body-scanners-safe/. The Transportation Security Administration (TSA) began implementing millimeter wave scanners in airports in 2010 in response to the notorious underwear bomber debacle in 2009. *See id*.; *see also* Michael Crowley, *Beware "Underwear 2": TSA Chief Offers Rare al Qaeda Bomb Details*, TIME (July 19, 2013), http://swampland.time.com/2013/07/19/beware-underwear-2-tsa-chief-offers-rare-al-qaeda-bomb-details/. For anyone who has encountered a millimeter wave scanner at an airport security checkpoint, they are "the ones you stand in with your feet apart and your hands above your head." Heid, *supra*. Unlike metal detectors, millimeter wave scanners also detect non-metal threats, such as plastic explosives. *Id.*

28. *See* MARY W. GREEN, NAT'L INST. JUST., THE APPROPRIATE AND EFFECTIVE USE OF SECURITY TECHNOLOGIES IN U.S. SCHOOLS 65 (1999).

29. *See id.* at 78–81.

watches can all potentially set off the alarm.[30] Because many weapons such as knives and guns are made of metal, metal detectors are also fairly effective at preventing weapons from passing through a security checkpoint undetected.[31]

Millimeter wave scanners, on the other hand, are becoming more controversial as evidence of their ineffectiveness continues to mount. In response to a TSA request for comments during its formal rulemaking process, many commenters expressed concern about the effectiveness of millimeter wave scanning devices at detecting weapons.[32] At least one report leaked from the Department of Homeland Security's Office of Inspector General in 2015 found that after the implementation of these devices, the TSA failed to detect explosives and handguns 96% of the time.[33] It is unclear how much of this failure percentage can be attributed to human operator error versus the millimeter wave scanners themselves.[34]

In contrast, the Patscan provides much more information than a metal detector and has a higher success rate than a millimeter wave scanner. Unlike metal detectors, the Patscan is capable of differentiating between benign metal objects and weapons.[35] Also, unlike the millimeter wave scanner, which may be failing to detect explosives and handguns up to 96% of the time, the Patscan has a "true positive" rate of 91.6%, meaning that it fails to detect potential weapons only 8.4% of the time.[36] The technology that allows the Patscan to positively identify concealed weapons raises serious privacy concerns. The specificity of the information that the Patscan can provide about a weapon is alarming. While a metal detector or millimeter wave scanner can merely indicate that an individual might be carrying a weapon, the Patscan affirmatively determines that an individual is carrying a weapon. The Patscan's ability to compare information from the scan against a database will reveal a large amount of information about the concealed weapon being carried by an individual.[37] For an individual legally carrying a concealed weapon, disclosure of the intimate details about their weapon to anyone with a Patscan installed on their property may be disconcerting.

There are several other differences between the Patscan and conventional security technologies. First, the Patscan does not require a direct line of sight; meaning that it can be installed covertly in walls, desks, floors, and other discreet areas.[38] It follows then, that if installed discreetly the Patscan could potentially allow security personnel to electronically search individuals who pass by the hidden Patscan device without their knowledge or cooperation. Metal detectors and millimeter

30. *See id.* at 78–79.

31. *See generally id.* at 65.

32. Passenger Screening Using Advanced Imaging Technology, 81 Fed. Reg. 11364, 11376–77 (2016).

33. *See Aviation Security Challenges: Is TSA Ready for the Threats of Today?: Hearing Before the Comm. of Homeland Sec.*, 114th Cong. (July 29, 2015) (opening statement of Michael McCaul, Committee Chairman, R-Texas); Jennifer Scholtes, *Price for TSA's Failed Body Scanners: $160 Million*, POLITICO (Aug. 17, 2015, 5:09 AM EDT), https://www.politico.com/story/2015/08/airport-security-price-for-tsa-failed-body-scanners-160-million-121385.

34. *See* Scholtes, *supra* note 33.

35. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10.

36. *See* PatriotOne, *Patscan CMR*, *supra* note 17.

37. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10.

38. *See id.*

wave scanners on the other hand require the cooperation of the individual to be searched because they must pass through the device to be scanned.[39] The potential for covert installation of the Patscan also raises privacy concerns because individuals passing by the device likely will be unaware that they are being scanned. Individuals who are being unwittingly scanned by the Patscan do not have a meaningful opportunity to avoid the search by choosing not to enter an area.

Also, unlike metal detectors and millimeter wave scanners, the Patscan does not require human operators.[40] Since the Patscan does not require human operators, security personnel can be refocused to where they are needed most rather than stuck with the tedious task of screening individuals as they enter a secured area. This also reduces the potential for human error in the screening process, which is a concern when using metal detectors and millimeter wave scanners.[41]

Furthermore, the Patscan itself does not generate an image of the person being scanned,[42] but a USB camera can be attached to the Patscan to take a picture of individuals who are positively identified as carrying a concealed weapon.[43] Metal detectors also do not generate an image of the person being scanned, but millimeter wave scanners were initially quite controversial because of privacy concerns raised by the detailed images generated of the body of the person being scanned.[44]

Finally, there will likely be a price difference between the Patscan and millimeter wave scanners. PatriotOne has not yet provided pricing for a single Patscan unit, but their promotional materials describe millimeter wave scanners as "expensive" and the Patscan as a less expensive alternative.[45] Millimeter wave scanners have an acquisition cost of about $175,000 per unit.[46] Metal detectors are about $10,000 per unit.[47] Depending on the price PatriotOne sets for Patscan, it may be a cost effective alternative to conventional security technology.

Overall, when considering effectiveness and price, PatriotOne has positioned its Patscan device in such a way that is likely to promote widespread adoption by

---

39. *See Current Technologies*, PATRIOTONE TECH., https://patriot1tech.com/threats/current-technologies/ (last visited Mar. 24, 2019).

40. *See* PatriotOne, *Data Sheet*, *supra* note 8.

41. *See, e.g.*, Scholtes, *supra* note 33 (discussing the possibility of human error contributing to at least part of the 96% failure rate of millimeter wave scanners).

42. *See* PatriotOne, *Data Sheet*, *supra* note 8.

43. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10.

44. *See* Julie Accardo & M. Ahmad Chaudhry, *Radiation Exposure and Privacy Concerns Surrounding Full-Body Scanners in Airports*, 7 J. RADIATION RES. APPLIED SCI. 198, 199 (2014) (explaining that the TSA was pressured to change millimeter wave scanners to produce less exposing images).

45. *See* PatriotOne, *Data Sheet*, *supra* note 8.

46. BART ELIAS, CONG. RES. SERV., R42750, AIRPORT BODY SCANNERS: THE ROLE OF ADVANCED IMAGING TECHNOLOGY IN AIRLINE PASSENGER SCREENING 3 (2012). While the acquisition cost of millimeter wave scanners is about $175,000 per unit, that amount only reflects the purchase price. The annual cost associated with deploying and operating millimeter wave scanners is roughly $655,000 per unit deployed. *Id.* at 3–4.

47. Security Magazine, *Millimeter Scanning at Airports: Is It Worth the Cost?*, SECURITY (Feb. 21, 2009), https://www.securitymagazine.com/articles/79508-millimeter-scanning-at-airports-is-it-worth-the-cost-1.

security forces around the world. Whether PatriotOne can successfully navigate the many obstacles faced by businesses attempting to launch products into the global marketplace remains to be seen. What is certain, however, is that the emergence of the Patscan, and the technology powering it, has created a new gap in the current landscape of Fourth Amendment jurisprudence. Having explained the basic features, design, and purpose of the Patscan, Part III of this note turns to the state action doctrine and the current Fourth Amendment landscape.

III. BACKGROUND ON THE FOURTH AMENDMENT AND STATE ACTION DOCTRINE

There are essentially three main parts to a search analysis under the Fourth Amendment. First, the challenged conduct must be evaluated under the state action doctrine, because most of the Constitution—including the Fourth Amendment—only applies to the government.[48] Second, if state action is present, it must be determined whether the challenged conduct constitutes a "search" within the meaning of the Fourth Amendment.[49] Finally, if the challenged conduct is a search, it will be evaluated for reasonableness.[50] Before explaining each of these steps in more detail, it is helpful to highlight the debate over what exactly the Fourth Amendment requires.

A. What Does the Fourth Amendment Require?

The Fourth Amendment provides that:

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

The Fourth Amendment consists of two clauses: the Reasonableness Clause, which requires that searches and seizures be reasonable, and the Warrant Clause, which, at a minimum, lays out the specific requirements of a valid warrant.[52] There is an ongoing debate about whether the two clauses are intended to be read as an interconnected whole or as two separate parts.[53] The warrant preference interpretation of the Fourth Amendment holds that the Warrant Clause is interrelated to the Reasonableness Clause, and in addition to setting the requirements for a valid

48. *See infra* Section III.B.
49. *See infra* Section III.C.
50. *See infra* Section III.D.
51. U.S. CONST. amend. IV.
52. Cynthia Lee, *Criminal Law: Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1413 (2010).
53. *Id.* at 1408–13.

warrant, also implies a warrant requirement.[54] Under this view, warrantless searches are *per se* unreasonable unless a warrant exception applies.[55]

More recently, another view that the Fourth Amendment contains two distinct and separate clauses, has regained some traction within the Supreme Court.[56] This separate clauses[57] approach to the Fourth Amendment was the competing view to the warrant preference approach for the first sixty years of the twentieth century.[58] Under this separate clauses view, the Reasonableness Clause and the Warrant Clause are completely independent and separated by the presence of the word "and" situated between them.[59] When interpreted under this view,

---

54. David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B. U. L. REV. 425, 427 (2016).

55. *Id.* at 426; *see also* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions.").

56. Lee, *supra* note 52. At least one recent Supreme Court Justice Scalia, advocated that the Court return to the separate clauses viewpoint. *See* California v. Acevedo, 500 U.S. 565, 581 (1991) (Scalia, J., concurring) ("The Fourth Amendment does not by its terms require a prior warrant for searches and seizures; it merely prohibits searches and seizures that are 'unreasonable.' What it explicitly states regarding warrants is by way of limitation upon their issuance rather than requirement of their use.").

57. The "separate clauses" approach is also commonly referred to as the "reasonableness view." Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L. J. 1133, 1139 (2012).

58. *See Acevedo*, 500 U.S. at 582. In his concurring opinion in *Acevedo*, Justice Scalia briefly explained the clash between the warrant preference view and the separate clauses view before advocating for the latter:

> Although the Fourth Amendment does not explicitly impose the requirement of a warrant, it is of course textually possible to consider that implicit within the requirement of reasonableness. For some years after the (still continuing) explosion in Fourth Amendment litigation that followed our announcement of the exclusionary rule in Weeks v. United States, 232 U.S. 383 (1914) (parallel citations omitted), our jurisprudence lurched back and forth between imposing a categorical warrant requirement and looking to reasonableness alone (internal citations omitted). By the late 1960s, the preference for a warrant had won out, at least rhetorically. (internal citations omitted).
>
> The victory was illusory. Even before today's decision, the "warrant requirement" had become so riddled with exceptions that it was basically unrecognizable. In 1985, one commentator cataloged nearly 20 such exceptions . . . . Since then, we have added at least two more . . . . Our intricate body of law regarding "reasonable expectation of privacy" has been developed largely as a means of creating these exceptions . . . .
>
> Unlike the dissent, therefore, I do not regard today's holding as some momentous departure, but rather as merely the continuation of an inconsistent jurisprudence that has been with us for years . . . . There can be no clarity in this area unless we make up our minds, and unless the principles we express comport with the actions we take.
>
> In my view, the path out of this confusion should be sought by returning to the first principle that the "reasonableness" requirement of the Fourth Amendment affords the protection that the common law afforded . . . .

Id. at 582–83.

59. *See* Lee, *supra* note 52, at 1413.

reasonableness becomes the only requirement for a constitutional search and the Warrant Clause does not require that searches and seizures be preceded by valid warrants.[60] Instead, the Warrant Clause only limits the circumstances under which warrants may be issued by requiring that warrants be based on probable cause supported by oath or affirmation and listed with particularity "the place to be searched, and the persons or things to be seized."[61]

On the surface, the debate appears to be settled in favor of the Fourth Amendment containing an implied warrant requirement.[62] However, underneath the surface a trend towards requiring only reasonableness undermines the implied warrant requirement. As Justice Scalia pointed out, the growing number of exceptions to the warrant requirement have rendered it nearly "unrecognizable."[63] While the Court has not expressly abandoned the warrant preference view, it has espoused that "the touchstone of the Fourth Amendment is reasonableness" with increasing frequency."[64] While doing so, it has continued to expand both the number and scope of the exceptions to the warrant requirement. These developments lend credence to the argument that in more recent Supreme Court Fourth Amendment cases, the Court only pays lip service to the implied warrant requirement before ultimately evaluating the search based on reasonableness.

The debate has become even more prominent as modern surveillance technology has been increasingly adopted by law enforcement.[65] Because it has chosen not to expressly adopt the separate clauses approach up to this point despite ample opportunity to do so, it seems unlikely that the Supreme Court will change course anytime soon. Yet, it also seems unlikely that the Court will diminish the warrant exceptions that it has already created. The solution to this jurisprudential morass is a topic worth consideration. But the lengthy discussion necessary to do it justice is outside the scope of this note.[66] This note will analyze the constitutionality of searches conducted using the Patscan through the lens of reasonableness, because that is the direction the Supreme Court appears to be trending.[67]

B. State Action Doctrine: Who Does the Fourth Amendment Apply To?

A preliminary question to ask when evaluating a set of circumstances through the lens of a Fourth Amendment claim is: who must comply with its requirements? The Fourth Amendment applies to both the federal government and to the states.[68] Generally, the Fourth Amendment only applies to actions of the states and the

60. *Id.* While a warrant is not required under the separate clauses view, the presence of a valid warrant prior to a search or seizure still has an impact on the reasonableness prong of the Fourth Amendment search analysis. *See infra* Section III.D. (discussing the reasonableness of searches).

61. *See* Lee, *supra* note 52 at 1413; U.S. CONST. amend. IV.

62. *See Acevedo*, 580 U.S. at 582; *see also supra* text accompanying note 58.

63. *Id.*

64. *See* Lee, *supra* note 5752, at 1143.

65. Gray, *supra* note 54, at 429.

66. For a more in-depth discussion of the separate clauses and warrant preference debate see Gray, *supra* note 57. *See also* Lee, *supra* note 52.

67. *See* Lee, *supra* note 52.

68. *See generally* Mapp v. Ohio, 367 U.S. 643 (1961) (holding that the Fourth Amendment applies to the states via the Due Process Clause of the Fourteenth Amendment).

federal government, whereas, generally the actions of private individuals do not implicate the Fourth Amendment.[69] This concept is known as the "state action" doctrine.[70] However, the actions of private individuals can become state action if the actions fall within one of the exceptions to the state action requirement.[71] Conceptually, the state action doctrine is not difficult to understand. In application, however, it is much more difficult to determine when private conduct may become state action.[72] There are two exceptions to the state action requirement that the Court appears to have settled on; the public function exception and the entanglement exception.[73] These two exceptions, when applicable, work to recharacterize the private party's actions as "state action," consequently requiring that the private party's conduct conform to the requirements of the Constitution.[74]

i. The Public Function Exception

The public function exception in its original form appeared fairly broad in scope. One of the first cases that helped create the public function exception was *Marsh v. Alabama*.[75] In *Marsh*, a police officer arrested a Jehovah's Witness in Chickasaw, Alabama, a private company-owned town, for standing on the sidewalk and distributing religious materials to people without a permit.[76] The town had "all the characteristics of any other American town," except that it was owned by the Gulf Shipbuilding Corporation.[77] The Court reasoned that the company town of Chickasaw was being allowed by the state of Alabama to oversee a community as if

69. Jackson v. Metro. Edison Co., 419 U.S. 345, 349 (1974). Professor Donald Crowley explains state action doctrine as follows:

> The state action doctrine ranks as one of the more illusive doctrines of constitutional law. As an abstract concept it is fairly easily explainable, but its application to actual situations is much more problematic. As a concept of federal constitutional law, the doctrine applies to the notion that constitutional rights act as restrictions on government actors but not private individuals, businesses, or groups. Thus, the ban against unreasonable searches restricts government intrusions into one's personal effects, but does not limit the ability of a snoopy neighbor to investigate your basement activities. While the neighbor might be subject to a trespassing charge, he cannot be held to have violated the Fourth Amendment.

Donald Crowley, *Student Athletes and Drug Testing*, 6 MARQ. SPORTS. L. J. 95, 100 (1995).

70. *Jackson,* 419 U.S. at 349–50.

71. *See* Crowley, *supra* note 69, at 103 (discussing the ways in which private action might become state action).

72. As one commentator from the 1990s put it, "State action is a sea in which everything else floats." C. Edwin Baker, *Private Power, the Press, and the Constitution*, 10 CONST. COMMENT. 421, 422 (1993). If state action is a sea, its waters are murky indeed.

73. *See Jackson*, 419 U.S. at 352.

74. *See* Sean D.G. Camacho, *Can You Hear Me Now? Time to Consider Whether Cell Phone Providers Are State Actors*, 49 SUFFOLK U. L. REV. 257, 261–62 (2016).

75. *Marsh*, 326 U.S. 501.

76. *See id.* at 502–04.

77. *Id.* at 502.

it were a public entity.[78] Creating the public function exception in perhaps its broadest form, the Court held that the U.S. Constitution was enforceable against the company town of Chickasaw because it was filling the role of a public entity.[79]

Later, courts including the Burger Court and Rehnquist Court increasingly narrowed the scope of the public function exception.[80] In 1974, the Court held that the public function exception applies when a private entity exercises a power that is "traditionally and exclusively reserved to the State."[81] In doing so, the Court narrowly applied the public function exception, holding that a private company providing electricity to citizens was not state action, despite heavy state regulation of the industry, because the service was not one the state had "traditionally" and "exclusively" provided.[82]

ii. The Entanglement Exception

The entanglement exception applies when the "state's involvement with [a] private party has been so pervasive that it significantly facilitates or supports the challenged actions of the private party."[83] For example, in *Burton v. Wilmington Parking Authority*, the Court held that the state was sufficiently involved with a discriminatory private actor when it leased a business space within a state-owned parking structure to the private actor.[84] The Court reasoned that the state's placement of its "power, property, and prestige" behind the discriminatory actions of the private actor were enough that the private individual's actions could not be considered "purely private."[85] While it is not always clear how and when the Court will find a government actor to be sufficiently entangled with the actions of a private individual, it is apparent that more government involvement is required than mere licensing, funding, or regulation of the private actions.[86]

78. *See* Camacho, *supra* note 74, at 260.

79. *See Marsh*, 326 U.S. at 509.

> "In our view the circumstance that the property rights to the premises where the deprivation of liberty, here involved, took place, were held by others than the public, is not sufficient to justify the State's permitting a corporation to govern a community of citizens so as to restrict their fundamental liberties and the enforcement of such restraint by the application of a State statute. Insofar as the State has attempted to impose criminal punishment on appellant for undertaking to distribute religious literature in a company town, its action cannot stand."

80. *See* Crowley, *supra* note 69, at 102.

81. *See* Jackson v. Metro. Edison Co., 419 U.S. 345, 352 (1974); *see also* Camacho, *supra* note 74, at 262.

82. *See Jackson*, 419 U.S. at 352–54. Interestingly, when laying out the traditional and exclusively reserved state test in *Jackson*, the Court relied upon four cases where it had applied the state action doctrine to private actors to hold their actions unconstitutional. *See* Nixon v. Condon, 286 U.S. 73 (1932) (election); Terry v. Adams, 345 U.S. 461 (1953) (election); Marsh v. Alabama, 326 U.S. 501 (1946) (company town); Evans v. Newton, 382 U.S. 296 (1966) (municipal park).

83. *See* Crowley, *supra* note 69, at 102.

84. Burton v. Wilmington Parking Auth., 365 U.S. 715, 716–17 (1961).

85. *Id.* at 725.

86. *See* Camacho, *supra* note 74. *See also* Moose Lodge No. 107 v. Irvis, 407 U.S. 163, 172 (1972) (holding that a state selling a liquor license to a privately-owned social club did not cause the state to be substantially involved in the private discriminatory actions of the club).

C. What is a Search for Purposes of the Fourth Amendment?

i. Evolution of Fourth Amendment Searches

The meaning of the word "search" as interpreted by the U.S. Supreme Court has evolved over time. In its early decisions, the Supreme Court's Fourth Amendment jurisprudence relied upon a property-rights based framework.[87] Under the property-rights based framework, a search occurs whenever the government physically intrudes upon a constitutionally protected area, such as trespassing upon an individual's property to obtain information.[88] The landmark case from the property-rights based era of Fourth Amendment jurisprudence is *Olmstead v. United States*.[89] In *Olmstead*, the Court explained that for a defendant to show his Fourth Amendment rights were violated there must have been "an official search and seizure of his person, or such seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[90] In other words, without a physical invasion of a constitutionally protected area such as his body or home, there simply could not be a search within the meaning of the Fourth Amendment.

The property-rights based framework was the dominant framework for a period spanning from the late-eighteenth century when the Fourth Amendment was ratified, up until the second half of the twentieth century.[91] In the 1960s, however, the Supreme Court began to move away from the property-rights based approach.[92] By 1967, two cases, *Warden v. Hayden* and *Katz v. United States*, marked what was thought to be the end of the property-rights based Fourth Amendment framework.[93] While *Warden* was decided first, *Katz* is often regarded as the seminal case marking the Supreme Court's departure from the property-rights approach to the Fourth Amendment.[94] In *Katz*, the Court tells us that "the Fourth Amendment

87. Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 23 (2015).

88. *Id.*

89. Olmstead v. United States, 277 U.S. 438, 465 (1928) (holding that wiretapping a telephone line outside of a defendant's house to intercept and listen to telephone calls coming from the telephone inside the house was not a search because the wiretapping was done without any physical intrusion onto his property).

90. *Id.* at 466.

91. *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 309, 320 (1998).

92. *See* Scott-Hayward, *supra* note 87, at 24.

93. *See* Clancy, *supra* note 91, at 320. *See generally* Warden v. Hayden, 387 U.S. 294 (1967) (eliminating the "mere evidence" distinction and rejecting the idea that property interests are the subject of the Fourth Amendment's protection); Katz, 389 U.S. 347 (1967).

94. *See, e.g.*, Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L. J. SCI. & TECH. 47, 55 (2014) (referring to Katz as a seminal decision); Seth Capper, *United States v. Jones and the*

protects people, not places" and that "[w]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection."[95] However, "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[96] Put another way, privacy, not property, is the subject of the Fourth Amendment's protection.[97]

Justice Harlan's famous concurrence in *Katz* gave us the test that has been used for the last fifty years by the Supreme Court in determining whether a search has occurred.[98] He said that the Fourth Amendment protects areas in which a person has a "reasonable expectation of privacy."[99] The test for determining whether a person has a reasonable expectation of privacy is twofold.[100] First, "a person [must] have exhibited an actual (subjective) expectation of privacy."[101] Second, "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[102] In cases following *Katz*, the Court further articulated the "reasonable expectation of privacy" test, explaining that the test has both a subjective prong and an objective prong.[103] Until 2012, Justice Harlan's two-pronged "reasonable expectation of privacy" test was the dominant method by which the Supreme Court determined whether a search had occurred within the meaning of the Fourth Amendment.

ii. Reinvigoration of the Property-Rights Based Framework

In *United States v. Jones*, the Supreme Court reinvigorated the property-rights based approach.[104] The Supreme Court further clarifies in *Jones* that *Katz* cannot have replaced the trespass test for determining whether a search has occurred because it is an "irreducible constitutional minimum."[105] Instead, *Katz* supplements the property-rights approach in cases where there has not been a physical trespass but an individual's expectation of privacy has nevertheless been invaded.[106] By replacing the property-rights based approach with the two-part framework from *Katz* and then reviving the property-rights approach in *Jones*, the Supreme Court appears to have come full circle in determining what constitutes a search under the Fourth Amendment. However, after nearly 200 years of attempting to define what a search is, the Court is not just back where it started. Instead of the pre-1967 property-rights approach being the *only* test for identifying a search, the Court now has two

---

Debate Over Warrantless GPS Surveillance on Vehicles, 2 ALA. C. R. & C.L. L. REV. 175, 179 (2011) (referring to Justice Harlan's concurring opinion in Katz as seminal).

95. *Katz*, 389 U.S. at 351.
96. *Id.*
97. Scott-Hayward, *supra* note 87, at 24.
98. *Id.* at 25.
99. *Katz*, 389 U.S. at 360.
100. *Id.* at 361.
101. *Id.*
102. *Id.*
103. *See, e.g.*, Smith v. Maryland., 442 U.S. 735, 740 (1979); *see also* Scott-Hayward, *supra* note 87, at 25 (explaining that the two-part test from Justice Harlan's concurrence "has become known as the 'reasonable expectation of privacy' test").
104. *See* Scott-Hayward, *supra* note 87, at 25.
105. *See Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).
106. *See id.* at 411–12.

frameworks working in tandem to afford the Fourth Amendment's protections to both *people and constitutionally protected places*.

In sum, after *Jones*, a search has occurred either when there has been an intrusion upon an individual's reasonable expectation of privacy (Katz), or when the government physically invades a constitutionally protected area for the purpose of obtaining information (Jones).[107] A determination that a search has taken place is only the first step in the analytical framework of the Fourth Amendment search analysis, however. Once *Katz* or *Jones* has been used to determine that a state action does indeed constitutes a search within the meaning of the Fourth Amendment, the next inquiry is reasonableness.

D. Only Unreasonable Searches are Proscribed

The Fourth Amendment does not prohibit all searches, rather, it only prohibits searches that are "unreasonable."[108] Whether a search is reasonable "depends on all of the circumstances surrounding the search . . . and the nature of the search . . . itself."[109] In other words, there is no talismanic approach to determining the reasonableness of a search. Instead, the Court must delve into the facts of each case to evaluate a search's reasonableness. The Court is not without guidance, however. Through its precedent, the Court has crafted a balancing test for assessing the reasonableness of a search.[110] Under this balancing test, a search's reasonableness is evaluated "by balancing its intrusion on [an] individual's Fourth Amendment interest against its promotion of legitimate governmental interests."[111]

As discussed above, the Supreme Court's view of the Fourth Amendment's requirements may be evolving.[112] But under current Fourth Amendment case law, "warrantless searches are *per se* unreasonable, except, of course, when they are not."[113] The best way to ensure the reasonableness of a search is to obtain a warrant and execute it properly. Ideally, the government would always obtain a warrant before conducting a search. But the reality is that in many circumstances waiting for a judicially approved warrant is not practical. Consequently, the government conducts many searches without first obtaining a warrant. In acknowledgement of the government's needs to search some individuals without waiting for approval of

---

107. *See id.* at 407; *Katz*, 389 U.S. at 361.

108. *See* U.S. CONST. amend. IV; Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 619 (1989); *see also* Carroll v. United States, 267 U.S. 132, 147 (1925).

109. *Skinner*, 489 U.S. at 619 (citing United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985)).

110. *See id.* (citing Delaware v. Prouse, 440 U.S. 648, 654 (1979)).

111. *See id.* (quoting *Prouse*, 440 U.S. at 654).

112. *See supra* Section II.A.

113. Groh v. Ramirez, 540 U.S. 551, 573 (2004) (Thomas, J., dissenting); *see also* Birchfield v. North Dakota, 136 S. Ct. 2160, 2173 (2016) (explaining that the warrant requirement "is subject to a number of exceptions").

a warrant, the Supreme Court has created nearly two dozen exceptions to the warrant requirement.[114]

The reasonableness of warrantless searches hinges primarily on whether they fit within one of the nearly two dozen exceptions to the warrant requirement. These exceptions operate by tipping the scale in favor of the government when the Court is balancing an individual's privacy interest against the government's needs.[115] The exception tips the scale either by reducing the privacy interests of the individual or by amplifying the government's needs.[116] One such exception, the administrative search exception, is likely to govern the use of the Patscan in some contexts.[117] Another exception, the special needs exception, will govern the use of the Patscan in schools.[118] Discussion of the administrative search exception and the special needs exception will be deferred to Section IV.C.

IV. CONSTITUTIONALITY OF PATSCAN SEARCHES

Under most circumstances, use of the Patscan is likely to be found constitutional under existing Fourth Amendment caselaw. This is because a narrowing of the state action doctrine precludes a full-fledged Fourth Amendment analysis in many cases. In the cases that do survive the state action doctrine expanding exceptions to the warrant requirement, too much weight is given to the government's interests, all but ensuring that use of the Patscan will be constitutional. In the first step of the analysis, the constitutionality of using the Patscan to scan people for weapons will depend, in part, on the security personnel behind the machine.[119] If the personnel using the Patscan are state actors, we move on to the second step of our Fourth Amendment analysis.[120] If not, the scan will not trigger the Fourth Amendment's protections.[121] Upon a finding of state action, we must then determine whether a scan from the Patscan is a search. If so, the search's constitutionality will depend upon its reasonableness.[122] If the scan is not a search, it will not implicate the Fourth Amendment.[123]

---

114. *See Acevedo*, 500 U.S. at 582–83 (Scalia, J., concurring).

115. *See Skinner*, 489 U.S. at 619–20 (citations omitted):

> In most criminal cases, we strike this balance in favor of the procedures described by the Warrant Clause of the Fourth Amendment. Except in certain well-defined circumstances, a search or seizure in such a case is not reasonable unless it is accomplished pursuant to a judicial warrant issued upon probable cause. We have recognized exceptions to this rule, however, 'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.' When faced with such special needs, we have not hesitated to balance the governmental and privacy interests to assess the practicality of the warrant and probable-cause requirements in the particular context.

116. *See id.*

117. *See infra* Section IV.C.i.

118. *See infra* Section IV.C.ii.

119. *See supra* Section III.B.

120. *See supra* Section III.B.

121. *See supra* Section III.B.

122. *See supra* Sections III.C–D.

123. *See supra* Section III.C.

A. Is Use of the Patscan State Action?

Whether using the Patscan to scan an individual for weapons qualifies as state action will, like nearly every other aspect of Fourth Amendment analysis, depend upon the circumstances. While the Patscan is still in the early stages of the product life cycle and is not yet widely available, it is not difficult to conceptualize potential applications for its use. Airports, schools, government buildings, sports stadiums, large event venues, casinos, restaurants, private clubs, and movie theaters are just a few possible applications. For the purpose of a state action analysis, the many circumstances in which the Patscan might be used can be categorized into three basic groups: purely private actors, quasi-state actors, and clear state actors.

The first category consists of circumstances where purely private actors utilize the Patscan. Due to the possible applicability of the entanglement and public function exceptions, this category is the smallest of the three.[124] Only when the conduct is purely private would use of the Patscan fall into this category. For example, there would be no state action if an individual installed the Patscan at the front door to his house. Use of the Patscan under these circumstances would not qualify as state action because there is little to no government involvement. Home security is not a service that has been "traditionally" and "exclusively" provided by the state. Nor can it reasonably be argued that the state substantially facilitates or supports an individual's conduct when he chooses to purchase and install the Patscan.[125] Private business owners installing the Patscan at their place of business would also fall into this category if another private party owned the building or property on which their business is located.[126] Private clubs, movie theaters, or restaurants all might fall into this category. Unless the private place of business, like the restaurant in *Burton*, contracted with the state or leased state property, it would be unlikely to qualify as state action.[127] Thus, by definition, when use of the Patscan is purely private, it does not qualify as state action and cannot violate the Fourth Amendment.

The second category consists of those circumstances where private actors are using the Patscan, and the state is intertwined with the private actors in a way that requires a state action doctrine analysis. The private actors under these

124. The entanglement and public function exceptions cause otherwise private conduct to be re-characterized as "state action." *See supra* Section III.B.

125. Perhaps, it could be argued that the state facilitates the individual's purchase of the Patscan by building roads or encouraging interstate commerce. But such an incidental facilitation of private conduct is not *substantial* and is not within the ambit of the entanglement exception. *See supra* Section III.B.2. and accompanying text; *see also* Moose Lodge No. 107 v. Irvis, 407 U.S. 163, 172 (1972) (holding that sale of a liquor license to a private organization was not *substantial* facilitation of private conduct).

126. *See, e.g.*, *Moose Lodge No. 107*, 407 U.S. 163, 172 (1972); *but see Burton*, 365 U.S. at 724–25 (explaining that a small private business such as a restaurant may still be a state actor when it engages in a mutually beneficial lease of a business space from the state).

127. *See Burton*, 365 U.S. at 723.

circumstances could be referred to as quasi-state actors.[128] Such circumstances will arise when security personnel operating the Patscan are doing so on private property and are privately employed but the state is still significantly involved in some fashion. Sports stadiums, large event venues, and casinos are some examples of places that may fit into this category. In these cases, the courts will apply the public function and entanglement exceptions to determine whether the actions of the private actor are considered state action.[129] A difference in holdings between two district courts regarding sports stadiums demonstrates how the courts have narrowed the state action doctrine over the past few decades.

In *Ludtke v. Kuhn*, the New York Yankees Clubhouse prohibited female reporters from entering the Yankees' locker room to interview players immediately after games.[130] A female reporter brought a discrimination claim against the New York Yankees and several other defendants, and one of the key issues was whether the clubhouse policy was state action.[131] The New York Southern District Court looked to the entanglement exception in holding that the policy was state action.[132] The court found it significant that the Yankee Clubhouse was leasing the portion of the stadium from the City of New York, which was the owner of the entire Yankees Stadium.[133] Comparing the case to *Burton*, the court emphasized the "symbiotic relationship" between the Yankee Clubhouse and the City of New York.[134]

In contrast, in *Stark v. Seattle Seahawks*, the Washington Western District Court held that private security forces conducting pat-down searches of fans entering the Seahawks' stadium was not state action.[135] Two fans, who were subjected to the pat-down searches, brought a civil action for deprivation of their Fourth Amendment rights pursuant to 42 U.S.C. § 1983.[136] This court also looked to the

---

128. Under *Burton*, such actors would undoubtedly be considered state actors. *See generally Burton*, 365 U.S. at 715.

129. *See supra* Section II.B.

130. Ludtke v. Kuhn, 461 F. Supp. 86, 87–88 (S.D.N.Y. 1978).

131. *Id.* at 87–88, 93. The other defendants included "Bowie Kuhn, Commissioner of Baseball; Leland MacPhail, President of the American League of Professional Baseball Clubs . . . The Mayor of the City of New York; The Commissioner of Parks and Recreation for the City of New York; and The Director of the Economic Development Administration of The City of New York." *Id.* at 88.

132. *Id.* at 93.

133. *Id.* The City of New York owned the stadium because it had exercised eminent domain to acquire it several years earlier. *Id.* at 92.

134. *Ludtke*, 461 F. Supp. at 93. The court further explained:

> The facts of the case at hand so nearly resemble those of Burton that there can be little doubt that state action exists . . . Here, as in *Burton*, the place where the discriminatory acts occurred is owned by the state (the City of New York) and leased pursuant to special legislative provisions to the Yankees. In this case, as in *Burton*, the facility involved is maintained and improved with the use of public funds. The Court noted in *Burton* that the relationship of the public and private entities in that case placed them in a relationship of interdependence. The same observation can be made on these facts, where the annual rentals to be paid to the City for use of the stadium depend directly on the drawing power of Yankee games, and the City has in turn invested substantial sums of public money to enhance that drawing power by modernizing and improving the stadium itself.

Id. at 93–94.

135. Stark v. Seattle Seahawks, No. C06-1719JLR, 2007 WL 1821017 (W.D. Wash. June 22, 2007).

136. This is known as a "Section 1983" claim. *See id.* at *1. *See also* 42 U.S.C. § 1983 (2012). The action was brought against several named defendants, including The Seattle Seahawks (NFL team), Football

entanglement exception in determining whether the private action could be fairly attributed to the state.[137] Just like in *Ludtke*, the plaintiffs pointed to evidence of a symbiotic relationship between the private actors and the Stadium Authority,[138] including the fact that the private actors leased the stadium from the Stadium Authority.[139] They also pointed to the fact that the Stadium Authority shared revenue with the private actors and had "an equity stake in the Seahawks."[140] But, relying on Supreme Court precedent, the court took a narrow approach to the state action doctrine, explaining that a symbiotic relationship is only shown when the specific action in question is mutually beneficial to both the state and private actors.[141] In the court's view, the entanglement exception did not apply because the Stadium Authority did not benefit from the pat-down searches.[142]

In light of this narrowing of the state action doctrine, it seems unlikely that the Court would find use of the Patscan in sports stadiums or similar venues to be considered state action so long as the security personnel are private employees and the facility is being leased by a private actor. The possible benefits of a scan from the Patscan are the same as those from a pat-down search. The purpose is to detect concealed weapons and protect the safety of everyone within the stadium or venue. If promoting the safety of patrons does not benefit the government owner of the facility simply because a private company has leased it from the government and employed its own private security personnel, then it is unlikely that use of the Patscan in this context would be considered state action. As long as the entanglement exception is narrowly construed to require that the specific actions being challenged be the source of the "symbiotic" relationship between the private and state actor, use of the Patscan in sports stadiums and similar venues likely is not state action.

The public function exception offers another possible route to a finding of state action, but it has been met with mixed results across jurisdictions. When a private security officer has plenary power to make arrests under state law, some jurisdictions have found that the authority makes him a state actor.[143] In circuits

---

Northwest (the owner of the Seahawks), First & Goal ("a Washington corporation that leases [the stadium] for the benefit of the Seahawks"), the Stadium Authority (a public entity that owns the stadium), and Lorraine Hine (the Chair of the Stadium Authority's Board of Directors). *Stark*, 2007 WL 1821017, at *1–2.

137. *Stark*, 2007 WL 1821017, at *7–8.

138. The Stadium Authority was a public entity created by The Stadium Act for the purpose of constructing, owning, remodeling, and operating the Seahawks Stadium. *Id.* at *1–2.

139. *Id.* at *4.

140. *Id.*

141. *Id.* at *5–6.

142. *Id.* at *6–7. One might argue that the Stadium Authority benefited from the pat-down searches because it made fans more likely to purchase tickets because it made them feel more secure. More ticket purchases would mean more revenue and an increase in the value of the Stadium Authority's equity stake. In fact, the plaintiffs did make that argument, but the court dismissed the apparent benefit as "pure speculation." *Stark*, 2007 WL 1821017, at *6.

143. *See, e.g.*, Romanski v. Detroit Entm't, L.L.C., 428 F.3d 629, 639 (6th Cir. 2005) (holding that plenary arrest authority transforms a private security guard into a state actor via the public function

that have held that private security forces were state actors, the courts reasoned that a private security officer with plenary arrest authority is serving a public function because police power is one "traditionally and exclusively" held by the state.[144] Of course, in those jurisdictions, the issue can probably be avoided entirely by simply not providing private security forces with plenary arrest authority. Instead, the private security officers can exercise their power to make a citizens' arrest without being considered state actors.[145] Absent a Supreme Court opinion addressing this split, a finding of state action under the public function exception may depend on the jurisdiction in which the private security forces with arrest authority are using the Patscan. This potential for a patchwork of jurisdictions holding that use of the Patscan by private security personnel either is or is not state action is less than desirable considering the fundamental constitutional rights at stake.

Finally, the third category consists of circumstances where state action is clearly present. Such circumstances arise when the security personnel operating the Patscan are themselves government agents. The Transportation Security Administration (TSA)[146] in airports, employees at state-run public schools, state and federal law enforcement officers, and security personnel in government buildings all fall into this category of state actors. When the Patscan is used under the circumstances that arise in this category, there is no question as to the presence of state action or the applicability of the Fourth Amendment.

B. Is Use of the Patscan a Search?

Regardless of the circumstances under which the Patscan is used, the method the device uses to scan an individual remains the same.[147] If using the Patscan to scan an individual in an airport is a search, so too is using the Patscan to scan someone in a sports stadium or on a street corner. The question then, is whether bouncing microwaves off an individual and interpreting the reflected waves to determine whether they are carrying a weapon constitutes a search.

i. Physical Trespass Test

A scan from the Patscan likely does not physically trespass upon constitutionally protected areas in the sense contemplated in *Jones* or *Olmstead*. The trespass and search at issue in *Jones* was the attaching of a GPS tracking device to the undercarriage of an individual's vehicle and the subsequent tracking of his location.[148] In holding that installment of the tracking device was a search, the Court

exception). *But see* United States v. Day, 591 F.3d 679, 688–89 (4th Cir. 2010) (disagreeing with the holding from *Romanski* and finding that plenary arrest authority alone is not enough to change a private citizen to a state actor).

144. *See Romanski*, 428 F.3d at 637, 651.

145. *See Day*, 591 F.3d at 689.

146. The Transportation Security Administration (TSA) is a federal agency created by Congress to handle security at airports and improve security for other modes of transportation. *See* Aviation and Transportation Security Act of 2001 §101, 49 U.S.C. §114(a), (d)–(e) (2012).

147. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10 (explaining how the Patscan operates to scan individuals).

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

emphasized the physical nature of reaching under the vehicle to place the tracking device.[149] In *Olmstead*, the Court held that wiretapping an individual's phone was not a search under the physical trespass test so long as the government agent did not step onto the individual's property (a constitutionally protected area) to tap the telephone line.[150] *Olmstead* illustrates the principle that not only must the act in question be physical in nature, it must also intrude upon a constitutionally protected area.[151] *Olmstead* likely would be decided differently if it were before the Court today, because the modern Court is equipped with both the physical trespass test and the "reasonable expectation of privacy" test from *Katz*.[152] But, *Olmstead* is still useful in illustrating the nature of the physical trespass test reinvigorated by *Jones*.

The Patscan is used to scan both an individual's body and those items that she is wearing or carrying.[153] An individual's "person" is one of the protected areas enumerated within the Fourth Amendment,[154] and "has . . . been extended to include clothing, items in pockets, undergarments, socks, and other extensions of the body."[155] The Court has not provided a universal definition of "effects,"[156] but it has held that parcels,[157] luggage,[158] and vehicles,[159] are all constitutionally protected "effects." The Court has also distinguished that effects are personal property, not real property.[160] Between the Court's slightly expansive interpretation of "person" and its holding that luggage and parcels are effects, it seems clear that at minimum, an individual's body and the objects she is wearing or possessing are constitutionally protected areas. Thus, when scanning an individual for concealed weapons, the Patscan is being used on the constitutionally protected areas contemplated by the Court.

The problem is that the scan conducted by the Patscan is not physical in nature. Unlike in *Jones* where the government agent physically intruded upon an individual's "effect" by reaching under the vehicle to attach a GPS tracking device, the Patscan merely sends and receives electronic signals, requiring no physical intrusion upon the individual's "person" or "effects."[161] Since the Patscan does not physically

149. *Id.* at 410–11.

150. *See Olmstead*, 277 U.S. at 464–66. Perhaps if the telephone line was owned by the defendant the wiretapping would have constituted a physical trespass in the eyes of the Court.

151. *See id.*

152. *See supra* Section III.C.ii.

153. *See* PatriotOne, *Product Demonstration Video*, *supra* note 10.

154. U.S. CONST. amend. IV (protecting "persons, houses, papers, and effects").

155. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 592 (2017).

156. Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection,* 125 YALE L. J. 946, 960 (2016).

157. United States v. Jacobsen, 466 U.S. 109, 144 (1984).

158. United States v. Place, 462 U.S. 696, 705–06 (1983).

159. *Jones*, 565 U.S. at 404.

160. Brady, *supra* note 156.

161. *Jones*, 565 U.S. at 404–05; PatriotOne, *Product Demonstration Video*, *supra* note 10.

intrude upon the individual's "person" or "effects," its electronic scans are not searches under the physical trespass test from *Jones*. Perhaps in anticipation of devices such as the Patscan, Justice Scalia explained in *Jones* that "[s]ituations involving merely the transmission of electronic signals without trespass . . . *remain* subject to *Katz* analysis."[162]

ii. Reasonable Expectation of Privacy Test

A scan from the Patscan is a search under the reasonable expectation of privacy test from *Katz*. The first prong of the test, that the individual has a subjective expectation of privacy, will almost always be satisfied by the fact that the individual carrying a concealed weapon chose to conceal it.[163] The second prong of the test is more complex. This prong of *Katz*, if interpreted literally, gives rise to a troublesome question. Can an individual ever have a reasonable, societally recognized expectation of privacy in the objects he carries into an area he knows is protected by security? While this question can be asked in the context of security at government buildings, sports stadiums, schools, or any other areas in which the Patscan might be used, airports are particularly useful in illustrating this concept.

In our post-9/11 world, everyone who has flown and many who have never flown understand that to get into the boarding area of an airport they will have to pass through a security checkpoint. The current routine is essentially the same at every airport and is easily described: arrive two hours before your flight, get in line at the security checkpoint, take off your shoes, empty your pockets into a bin, get out your laptop or iPad and put it in a separate bin, place your bag on the conveyer belt to be x-rayed, and walk through the metal detector or millimeter wave machine. If a man walks into an airport expecting to get on a plane and he is carrying a revolver in his briefcase, we, as a society, expect him to be discovered. Substitute out the metal detector or millimeter wave machine for the Patscan, and that expectation does not change. Assuming all of this is true, how could we possibly conclude that society is prepared to recognize the man's expectation of privacy as reasonable?

The courts, even before 9/11, acknowledged that interpreting *Katz* in this way leads to problematic results.[164] In response to the government's assertion that an individual could not have "a reasonable expectation of privacy" in his carry-on luggage, the Ninth Circuit Court of Appeals reasoned:

> [The second requirement from *Katz*] does not mean that any kind of governmental intrusion is permissible if it has occurred often enough. The government could not avoid the restrictions of the Fourth Amendment by notifying the public that all telephone lines will be tapped, or that all homes will be searched. 'Airport searches' are not outside the Amendment simply

162. *Jones*, 565 U.S. at 411 (emphasis in original).

163. *See, e.g.*, United States v. Davis, 482 F.2d 893, 905 (9th Cir. 1973) (discussing whether the first requirement of the *Katz* test is met: "Clearly the first requirement was satisfied in this case: appellant relied on the privacy of his briefcase to conceal his gun.").

164. *See generally Davis*, 482 F.2d at 905 (declining to interpret the second prong of the reasonable expectation of privacy test in this manner); United States v. Albarado, 495 F.2d 799, 806 (2d Cir. 1974) (explaining that the concept has "little analytical significance").

> because they are being conducted at all airports. In none of the Supreme Court decisions excluding searches or seizures from the Fourth Amendment on the authority of *Katz* was the result based on such a rationale. Rather, in each case the individual's alleged reasonable expectation of privacy was negated on some other, independent, ground.[165]

In other words, society's reasonable expectations of privacy cannot be diminished simply because the governmental intrusions are common or recurring. Other circuits have discussed this issue in a comparable manner.[166] After 9/11, the cogency of this line of reasoning is even more evident. While the threat of hijacking and terrorism do have an impact on the Fourth Amendment search analysis, that impact is on the part of the analysis focused on the *reasonableness* of a search, not whether a search has occurred in the first place. Thus, whether in an airport, or passing through security anywhere else, an individual still has an objective expectation of privacy when it comes to the items he has concealed on his body or in his luggage.[167] Since both the subjective and objective prongs of the reasonable expectation of privacy test are met when an individual is screened by security, use of the Patscan to conduct that screening is a search within the meaning of the Fourth Amendment.

An additional ground for finding that use of the Patscan to scan individuals for concealed weapons constitutes a search can be found in the treatment of metal detectors by the circuit courts. In *United States v. Epperson*, the Fourth Circuit Court of Appeals concluded that use of a metal detector was a search when it was used to scan an individual about to board a plane.[168] The court in *Epperson* did not engage in the two-part analysis described in *Katz*.[169] Instead, the court stated simply that using a metal detector, "a government officer, without permission, discerned metal on Epperson's person."[170] The court went on to explain that "the very purpose and function of a [metal detector]: [is] to search for metal and disclose its presence in areas where there is a normal expectation of privacy."[171] Numerous

---

165. *Davis*, 482 F.2d at 905.

166. *See, e.g.*, United States v. De Los Santos Ferrer, 999 F.2d 7, 9 (1st Cir. 1993) ("We think that the Fourth Amendment issue is a difficult one. To be sure, a traveler who has any experience knows that luggage at airports is now commonly x-rayed for guns or explosives and that requests at the checkpoint to open the luggage are not uncommon. At the same time, these are administrative searches conducted for a limited purpose and this limited—and exigent—purpose has been the basis for allowing the searches en masse, without a warrant and without probable cause. There is at least some basis for concern about the government's falling-domino approach, by which each intrusion diminishes privacy expectations enough to permit a further infringement.").

167. *See Davis*, 482 F.2d at 905 (explaining that the second part of the *Katz* test is satisfied); *Albarado*, 495 F.2d at 802–03 (determining that screening a person and his luggage is a search whether done manually, with a metal detector, or with an x-ray).

168. United States v. Epperson, 454 F.2d 769, 770 (4th Cir. 1972), *cert. denied*, 406 U.S. 947.

169. *See id.*

170. *Id.*

171. *Id.*

opinions from the other circuits cite to *Epperson* for this principle without engaging in the reasonable expectation of privacy analysis themselves.[172]

The reasoning applied to metal detectors in *Epperson* seemingly could be applied to the Patscan as well. Like a metal detector, whose purpose and function "is to search for metal and disclose its presence in areas where there is a normal expectation of privacy," the Patscan's purpose and function is to search for weapons and disclose their presence in areas where there is a normal expectation of privacy.[173] In other words, metal detectors search for metal, the Patscan searches for weapons, and both are considered "searches" within the meaning of the Fourth Amendment.

C. Is Using the Patscan to Search an Individual Reasonable?

Turning to the reasonableness portion of our analysis, only the third category of circumstances, where there are clear state actors, need be evaluated. As explained in Part IV.A., sports stadiums, large event venues, casinos, restaurants, private clubs, and movie theaters are all possible places for the Patscan to be used that likely would fall outside the bounds of the state action doctrine's exceptions in their current form. Even if the government owns the property on which the private business is located and leases it to a private actor, enforcement of security using the Patscan, or otherwise, is outside the scope of the entanglement and public function exceptions in all but a very limited number of circumstances.[174]

The sections below analyze use of the Patscan for reasonableness in those circumstances where clear state action is present. Presumably, the government will not have obtained a warrant in any of the situations in which the Patscan might be used to search individuals. Therefore, reasonableness of the Patscan search will depend primarily on how well it fits within one of the exceptions to the warrant requirement.[175] The two exceptions that are most applicable in the context of the Patscan are the administrative search and special needs exceptions. In both contexts, we will see that the courts have given substantial weight to the government's goal of preventing violence.

---

172. *See Albarado*, 495 F.2d at 803 ("Even the unintrusive [metal detector] walk-through is a search in that it searches for and discloses metal items within areas most intimate to the person where there is a normal expectation of privacy.") (citing *Epperson*, 454 F.2d at 770); United States v. Slocum, 464 F.2d 1180, 1182 (3d Cir. 1972) ("The short answer to defendant's challenge directed against use of the [metal detector] is provided by United States v. Epperson . . . ."); Horton v. Goose Creek Independent Sch. Dist., 690 F.2d 470, 478 (5th Cir. 1982) (quoting *Epperson*, 454 F.2d at 770); United States v. Henry, 615 F.2d 1223, 1227 (9th Cir. 1980) (comparing x-rays and metal detectors and determining that both are searches); United States v. Vega-Barvo, 729 F.2d 1341, 1346–47 (11th Cir. 1984) (stating that scans with a metal detector have been "deemed a Fourth Amendment search") *cert. denied,* 469 U.S. 1088 (1984).

173. *See* PatriotOne, *Patscan CMR*, *supra* note 17.

174. Those circumstances being when the challenger can prove that enforcement of security directly benefits the government actor, *see supra* note 142 and accompanying text, which is unlikely in most cases, or in some jurisdictions where it has been held that private security officers with plenary arrest authority granted by the state are considered state actors via the public function exception, *see supra* note 143 and accompanying text, which is easily avoided.

175. *See supra* Section III.D.

i. The Administrative Search Exception

An administrative search is a search "conducted as part of a general regulatory scheme in furtherance of an administrative purpose, rather than as part of a criminal investigation to secure evidence of crime[.]"[176] Such a search may be permissible notwithstanding a lack of probable cause.[177] To be constitutional, administrative searches must be reasonable within the meaning of the Fourth Amendment.[178] "Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."[179] But an administrative search should be "as limited in its intrusiveness as is consistent with satisfaction of the administrative need that justifies it."[180]

a. Airports

The Supreme Court has not addressed whether the administrative search exception applies to searches made at security checkpoints in airports. Nor has it ruled specifically on whether the use of a metal detector or millimeter wave scanner to search individuals in airports is reasonable. However, the circuit courts have held that use of a metal detector in an "airport screening search" is constitutionally reasonable under the administrative search exception.[181] The airport screening search is an administrative search because it is "conducted as part of a general regulatory scheme in furtherance of an administrative purpose," that purpose being to "prevent the carrying of weapons or explosives aboard aircraft, and thereby to prevent hijackings."[182]

Looking to the first half of the balancing test, the government's need to search individuals for weapons in airports is quite clear. In 1973, the Ninth Circuit joined several other circuits in determining that "the [government's] need to prevent airline hijacking is unquestionably grave and urgent."[183] In our post 9/11 world, the government's need to prevent weapons or explosives from being brought aboard aircraft is even more pressing.[184]

176. United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973).

177. *Id.*

178. *Id.* at 910.

179. *Id.*

180. *Id.*

181. *See, e.g.*, *id.* at 912; United States v. Aukai, 497 F.3d 955, 960–62 (9th Cir. 2007) (overruling the part of *Davis* that requires consent, implied or express, for constitutional airport searches, but otherwise reaffirms that airport searches are reasonable).

182. *See Aukai*, 497 F.3d at 960 (quoting United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973)).

183. *Davis*, 482 F.2d at 910. *See also* United States v. Slocum, 464 F.2d 1180, 1182 (3d Cir. 1972); United States v. Bell, 464 F.2d 667, 669 (2d Cir. 1972); United States v. Epperson, 454 F.2d 769, 771 (4th Cir. 1972).

184. *See Aukai*, 497 F.3d at 960–61.

As for the other side of the balancing test, the courts have looked to the capabilities of "current technology" when evaluating the search's intrusiveness.[185] Because of the government's pressing need for airport searches, they have been held constitutionally reasonably provided they are "no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives . . . [and are] confined in good faith to that purpose."[186] In this respect, the Patscan may actually have a distinct advantage over the conventional metal detector and the millimeter wave machine. The Patscan is more precise than a metal detector because it only detects weapons and explosives, whereas metal detectors detect all kinds of metal objects and millimeter wave machines are intended to detect all concealed objects.[187] It could be argued that this increased precision makes the Patscan search less extensive than a search using a metal detector or millimeter wave machine. At any rate, the government's overwhelming need to prevent the hijacking of aircraft means that use of the Patscan to search people for weapons and explosives in an airport is, in all likelihood, reasonable and constitutional.

b. Government Facilities or Buildings

The administrative search exception's applicability to government buildings, such as courthouses, capitol buildings, and city halls, is substantially the same as it is to airports. The government has a legitimate goal, distinct from general crime prevention, of "prevent[ing] destruction and injury in government facilities."[188] The fact that the Patscan only searches for weapons and explosives means that in theory it is less intrusive than alternatives, such as metal detectors and pat-down searches. Thus, similar to airports, the government's interest in preventing destruction and injury outweighs the potential invasion of privacy.

ii. The Special Needs Exception in Public Schools

The Supreme Court has stated that warrantless searches that are not supported by probable cause can still be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[189] The Court has also held that such "special needs" are present in the context of public schools.[190] When applying the special needs exception, a balance must be struck between the students' legitimate expectations of privacy and the legitimate need for schools to maintain order and a safe learning environment.[191] In striking this balance, the court must look at "(1) the nature of the privacy interest upon which the search intrudes; (2) the character of the intrusion, [including] . . . whether the invasion of privacy is minimal or significant, and

185. *Id.* at 962.
186. *Id.*
187. *See supra* Section II.B.
188. *See* United States v. Kerr, 268 F. Supp. 3d 1125, 1128 (E.D. Wash. 2017).
189. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).
190. *Id.*
191. New Jersey v. T.L.O., 469 U.S. 325, 339–40 (1985).

(3) the nature and immediacy of the governmental concern at issue, and the efficacy of the means for meeting it."[192]

In *Vernonia*, the Supreme Court upheld a urinalysis drug test that was part of a district-wide drug policy authorizing random drug tests of student athletes.[193] The students were found to have diminished privacy interests because of their status as public-school students.[194] As for the character of the intrusion, the collection of urine samples was not a significant invasion of privacy because it was done in the privacy of a restroom and the samples were screened only for drugs, not underlying medical conditions of the students.[195] Finally, the nature of the concern, deterring drug use by schoolchildren, was important if not compelling.[196]

The Supreme Court has not ruled specifically on the reasonableness of using of a metal detector or millimeter wave scanner to conduct entry searches in schools. Although, some states have taken matters into their own hands. Tennessee has expressly authorized the use of metal detectors in schools through a statute.[197] State courts in New York, Pennsylvania, Illinois, Florida, and California have approved the use of metal detectors in schools.[198] In *People v. Pruitt*, an Illinois appeals court addressed the issue of metal detector searches in schools.[199] The court in *Pruitt* emphasized that the intrusiveness of requiring students to pass through a metal detector is minimal because it did not involve any physical touching.[200] As to the government's needs, the court held that the school's "special needs" included preventing violence in schools.[201] In doing so, the court reflected on the loss of innocence in schools that its holding represented:

> We long for the time when children did not have to pass through metal detectors on their way to class, when hall monitors were other children, not armed guards, when students dressed for school without worrying about gang colors. Those were the days when sharp words, crumpled balls of paper, and, at worst, the bully's fists were the weapons of choice.[202]

However, the court went on to state: "[j]udges cannot ignore what everybody else knows: violence and the threat of violence are present in the public schools."[203] Ultimately, in balancing the privacy interest of the student and the school's "special

192. People v. Pruitt, 662 N.E.2d 540, 543 (Ill. 1996) (citing *Vernonia*, 515 U.S. at 654–63).
193. *Vernonia*, 515 U.S. at 664–65.
194. *Id.* at 656–57.
195. *Id.* at 658–60.
196. *Id.* at 661.
197. TENN. CODE ANN. § 49-6-4207 (2017).
198. *See* Robert S. Johnson, *Counterpoint: Metal Detector Searches: An Effective Means to Help Keep Weapons Out Of Schools*, 29 J.L. & EDUC. 197, 202 (2000).
199. *See* People v. Pruitt, 662 N.E. 2d 540 (1996).
200. *Id.* at 547.
201. *See id.* at 545 (citing *T.L.O.*, 469 U.S. at 339.
202. *Id.*
203. *Id.* at 546.

need" to prevent violence, the court held that the suspicionless metal detector search did not violate the Fourth Amendment.[204]

While the Illinois Appeals Court has limited jurisdiction, its analysis of the use of metal detectors in schools is still instructive on the issue of implementing Patscan searches in public schools. The reduced privacy interest of public school students and the "special need" for prevention of violence in schools remain the same. The Patscan is similar to a metal detector in the fact that neither device requires a physical touching of the student during the search. Under this line of reasoning, replacing the metal detector with the Patscan likely would not change the outcome of *Pruitt*. Thus, a limited number of jurisdictions have likely already found that a search using a device such as the Patscan to screen students for weapons is reasonable under the Fourth Amendment. Based on the Supreme Court's finding that urinalysis drug testing of students was reasonable in light of the government's special need to prevent students from using drugs, it seems likely that the Court would also uphold the use of the Patscan given the government's special need of preventing violence in schools.[205]

V. CONCLUSION

Security technology is going to continue to advance, both in sophistication and capability. The Patscan is just an example of the incredible advancements technology has made in the first part of the twenty-first century. This relatively small device has the potential to revolutionize the look and feel of security checkpoints as we know them. With the enhancement of security technology, however, comes the increased risk of intrusions on the right to privacy. And the current jurisprudential landscape is filled with pitfalls, capable of undermining privacy rights in the face of new technology. The narrowing of both the public function exception[206] and entanglement exception[207] to the state action requirement is one such danger. As technology advances, the blurred lines between state and private actors will become increasingly important. A robust state action doctrine would subject quasi-state actors to the strictures of the Fourth Amendment, ensuring that privacy interests are at least balanced against government and security interests. A murky and narrow state action doctrine will serve to allow private security forces, equipped with advanced security technology such as the Patscan, to search individuals regardless of whether the government could constitutionally do so. Private security officers and guards already outnumber sworn law enforcement officers more than two to one.[208] Advanced security technology will put a large amount of power in their hands. Because of a narrow state action doctrine, they will be predominately unrestricted by the Fourth Amendment.

As for Fourth Amendment jurisprudence itself, the Court has created a patchwork of recognized privacy interests in the context of new technologies. But the

204. *Id.* at 547.

205. *See Acton*, 515 U.S. at 661; *T.L.O.*, 469 U.S. at 339.

206. *See supra* Section III.B.i.

207. *See supra* Section III.B.ii.

208. *See* Amy Goldstein, *More Security Firms Getting Police Powers/Some See Benefits to Public Safety, But Others Are Wary*, SFGATE (Jan. 7, 2007), https://www.sfgate.com/news/article/More-security-firms-getting-police-powers-Some-2625549.php.

creeping expansion of the number and scope of exceptions to the warrant requirement threatens to swallow the Fourth Amendment and its protections. As the twenty-first century progresses, the Patscan and other advancements in technology will continue to make the world a safer place. But they will also strain our current understanding of the right to be free from unreasonable searches under the Fourth Amendment. Justice Scalia was right: "[t]here can be no clarity in this area unless we make up our minds, and unless the principles we express comport with the actions we take."[209] If "the ultimate touchstone of the Fourth Amendment is reasonableness,"[210] perhaps it is time to reconsider our sacrificing of privacy for the sake of security. For "privacy erodes first at the margins, but once eliminated, its protections are lost for good, and the resultant damage is rarely, if ever, undone."[211]

209. California v. Acevedo, 500 U.S. 565, 583 (1991).

210. Riley v. California, 134 S. Ct. 2473, 2482 (2014) (quoting Brigham City v. Stuart, 547 U.S. 383, 403 (2006)).

211. United States v. Kincade, 379 F.3d 813, 871 (9th Cir. 2004).