TECHNOLOGICAL UBIQUITY AND THE EVOLUTION OF FOURTH AMENDMENT RIGHTS

ABSTRACT

This Note examines past Fourth Amendment jurisprudence in an effort to show the ways in which legal tests have had to adapt—and will need to continue adapting—to changes in the technology and surveillance methods used by law enforcement. The Note also discusses the arguably alarming degree to which law enforcement's surveillance arsenal has escalated. Local police departments now have resources like unmanned aerial vehicles (UAVs) and large networks of surveillance cameras at their disposal. Meanwhile, federal law enforcement and intelligence agencies like the National Security Agency are watching and collecting data on many forms of electronic communication all over the world.

The technology being used by law enforcement grows ever more sophisticated and ubiquitous. Legal decision makers must ensure that they adapt the law in a way that meets the challenges created by this technology while maintaining the Fourth Amendment as the bulwark that it has always been.

TABLE OF CONTENTS

I. INTRODUCTION

This Note examines the effects that modern technology has had on Fourth Amendment rights and jurisprudence. More specifically, this Note covers cases involving searches of computers and various forms of electronic communication, as well as GPS surveillance cases.[1] Each of these topics is academically well-trodden ground, but the term "technology" encompasses far more than computers and GPS devices. To be sure, the advancement of technology has forced courts to innovate their pronouncements of Fourth Amendment rights.[2] Although the principal goal of this Note is to inform, this Note also argues that technological trends in general society and in law enforcement circles are cause for concern in this area of law.[3] Indeed, this Note is not only about the ways in which technology has changed; it also aims to discuss the ways in which law enforcement uses of technology have changed.[4]

This Note does not substantially address the considerable body of statutory law involving electronic surveillance. Instead, this Note is concerned only with the Fourth Amendment. Although those statutes are important, they are beyond the scope of this Note.

Much ink has been spilled about the Fourth Amendment over the years, but much more may be needed in order to solve the problems technology poses to constitutional interpretation. This Note does not mean to set forth a grand, unified solution to these problems. It aims instead to define them and to discuss different ways of analyzing them.[5]

II. AN OVERVIEW OF THE DEVELOPMENT OF TECHNOLOGICAL FOURTH AMENDMENT JURISPRUDENCE

Fourth Amendment jurisprudence is highly varied, particularly in the factual situation of each case. Moreover, Fourth Amendment cases, like cases in so many other areas of law, build on each other over time. Discussing and analyzing just one case is not enough to show where the law is headed or from where it came.

1. *See infra* Parts II.B, III.
2. *See infra* Parts II, III.A.
3. *See infra* Parts III.D, IV.
4. *See infra* Part IV.
5. *See infra* Part III.

A. *From Where It Came*

Studying the origins of a given field is perhaps the best way to illuminate the direction that field is traveling. Since the body of Fourth Amendment jurisprudence is vast and complex, it is most instructive to start with the basics. The Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[6] Cases deciding what constitutes a "search," what constitutes a "seizure," and whether the search or seizure is "unreasonable" are legion.

This amendment is said to protect a certain right to personal privacy ("[t]he right of the people to be secure").[7] Of course, it is not difficult to see how technology has changed Americans' idea of what can be considered "private." If a person writes something on the Internet and attaches one's name to the statement—as in a blog entry or a Facebook status update—then he or she can expect that statement to appear when someone searches the writer's name via Google or some other search engine. On the other hand, people generally expect certain communications, such as e-mails and text messages, to be kept private, viewed only by the sender and the recipient. The most important Fourth Amendment cases of the past obviously do not contemplate this relatively new technology. However, a careful examination of the case law shows that, even though the technology has changed, the same sorts of problems have recurred.

The question, as in *Katz v. United States*,[8] often boils down to considerations of privacy. Justice Harlan, in a concurring opinion in *Katz*, famously articulated the standard that a person must have "an actual (subjective) expectation of privacy . . . [,] one that society is prepared to recognize as 'reasonable'" in order to trigger Fourth Amendment protection.[9] Although this is the best-known point of *Katz*, the case bears closer inspection.

Federal agents used an electronic listening device to eavesdrop on Katz's conversations in a public phone booth.[10] Rather than frame the dispute as a question of whether the phone booth was a "constitutionally

6. U.S. CONST. amend. IV.
7. *Id.*
8. Katz v. United States, 389 U.S. 347 (1967).
9. *Id.* at 361 (Harlan, J., concurring).
10. *Id.* at 348 (majority opinion).

protected area," the majority emphasized that "the Fourth Amendment protects people, not places."[11] The Fourth Amendment, therefore, does not protect "[w]hat a person knowingly exposes to the public," but it does protect "what he seeks to preserve as private, even in an area accessible to the public."[12] In defining what Katz sought to keep private by entering the phone booth, the Court did not consider the transparency of the booth to be relevant because Katz wanted to shut out prying ears, not prying eyes.[13] Because the listening device heard and recorded exactly what Katz justifiably wanted to keep private, the Government's eavesdropping violated Katz's privacy and was a Fourth Amendment search and seizure.[14] Although Justice Harlan's concurrence arguably articulated it better, the test the *Katz* majority used looks substantially similar to the one Justice Harlan set forth.[15]

A large body of case law has developed over the years since *Katz* regarding police officers' use of various electronic devices in surveillance of suspects.[16] These cases have significantly expounded on the interaction between technology and the Fourth Amendment. *Smith v. Maryland* is a seminal example.[17] In *Smith*, the police (via Smith's phone company) used a device called a pen register to record the numbers dialed from Smith's

11. *Id.* at 351 (internal quotation marks omitted). This statement is true to the text of the Fourth Amendment, which protects "[t]he right of *the people* to be secure . . . against unreasonable searches and seizures." U.S. CONST. amend. IV (emphasis added).

12. *Katz*, 389 U.S. at 351–52.

13. *Id.* at 352. As the Court noted, "[o]ne who occupies [the booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Id.*

14. *Id.* at 353.

15. *Compare id.* ("The Government's activities in electronically listening to and recording [Katz's] words violated *the privacy upon which he justifiably relied* while using the telephone booth . . . ." (emphasis added)), *with id.* at 361 (Harlan, J., concurring).

16. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 29–30 (2001) (detailing police use of a thermal-imaging device to investigate defendant's home); United States v. Vela, 486 F. Supp. 2d 587, 589–90 (W.D. Tex. 2005) (discussing whether a federal agent's use of night vision goggles constituted a search of the defendant's car). For a thorough discussion of *Kyllo*, see *infra* notes 53–64 and accompanying text, and for a more thorough discussion of *Vela* and how it is distinguished from *Kyllo*, see *infra* Part III.A.

17. Smith v. Maryland, 442 U.S. 735 (1979).

home phone.[18] Using information gathered via the pen register and other means, the police were able to obtain a search warrant for Smith's home.[19] *Smith* differed from *Katz* in that pen registers, unlike listening devices, "do not acquire the *contents* of communications."[20] Ultimately, the Supreme Court rejected Smith's argument that he had a legitimate expectation of privacy in the numbers he called from his phone.[21] The privacy right Smith asserted against the use of the pen register did not meet the subjective prong of the *Katz* test because the numbers dialed were voluntarily disclosed to the phone company.[22] The Court presumed this point to be common knowledge among phone users.[23] Even if Smith had a subjective expectation of privacy in the phone numbers he dialed, it would not have been an expectation that society would recognize as reasonable.[24] The Court noted its consistent refusal to recognize a legitimate expectation of privacy in information voluntarily disclosed to third parties.[25] In disclosing the numbers he dialed to the phone company, Smith "assumed the risk that the company would reveal to police the numbers he dialed."[26]

United States v. Knotts was also significant; it reaffirmed the rule that police investigators can use technology to obtain information they would have otherwise been able to obtain in a lawful manner.[27] In *Knotts*, a chemical company told police that one of its former employees had been stealing its chemicals and possibly using them to make illegal drugs.[28] Visual observation revealed that the former employee, Tristan Armstrong, had been subsequently buying similar chemicals from another chemical company.[29] Officers, after obtaining consent from the seller, placed a tracking device inside a container of chloroform, which Armstrong later

18. *Id.* at 737.
19. *Id.*
20. *Id.* at 741.
21. *Id.* at 742.
22. *Id.* The Court also pointed out that phone companies themselves use pen registers in the course of normal business. *Id.*
23. *See id.* ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").
24. *Id.* at 743.
25. *Id.* at 743–44.
26. *Id.* at 744.
27. United States v. Knotts, 460 U.S. 276, 282 (1983).
28. *Id.* at 278.
29. *Id.*

bought.[30] Armstrong transported the container to the house of Darryl Petschen, an accomplice, and the container was put into Petschen's vehicle.[31] Officers then tracked the container to Knotts's cabin.[32] Based on visual surveillance and the location information obtained via the tracking device, the police obtained a warrant to search the cabin.[33] The search revealed an extensive drug laboratory and the container of chloroform in which the tracking device had been placed.[34]

The Supreme Court, in applying the *Katz* test, noted that the expectation of privacy in a motor vehicle is somewhat diminished.[35] Someone who is driving in a car on public roads "has no reasonable expectation of privacy in his movements from one place to another."[36] Moreover, as a motorist driving on public roads, Petschen "voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."[37] Knotts's argument focused on the fact that the police used the beeper to determine the container's location at his cabin.[38] However, the police did not use the beeper after the signal became stationary at Knotts's cabin.[39] There was "no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin."[40] Therefore, the Court held that police officers' monitoring via the beeper did not invade a reasonable expectation of privacy, and there was not a search or seizure under the Fourth Amendment.[41]

Shortly after *Knotts*, the Supreme Court fleshed out its surveillance jurisprudence in *United States v. Karo*.[42] An informant told Drug

30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.* at 279.
34. *Id.*
35. *Id.* at 281.
36. *Id.*
37. *Id.* at 281–82.
38. *Id.* at 284.
39. *Id.* at 284–85.
40. *Id.* at 285.
41. *Id.*
42. United States v. Karo, 468 U.S. 705 (1984).

Enforcement Administration (DEA) agents about a large order Karo and his associates had placed with him for ether.[43] DEA agents, with an authorizing court order and the informant's consent, surreptitiously placed a tracker in one of the cans of ether.[44] The agents eventually traced the tracking device to a house.[45]

The Court held that installing the tracking device did not infringe upon Karo's Fourth Amendment rights.[46] However, the Court held that monitoring the tracker's signal while the tracker was in a private home *did* violate "the Fourth Amendment rights of those who ha[d] a justifiable interest in the privacy of the residence."[47] The agents overstepped their bounds because they used the tracker several times after it came to rest at the house, thereby "obtain[ing] information that [they] could not have obtained by observation from outside the curtilage of the house."[48]

Knotts and *Karo* are significant because they drew a line in the sand; surveillance in a private residence is a Fourth Amendment violation, while surveillance on a public road is not.[49] These cases seem to evoke the idea of "constitutionally protected areas."[50] Regardless of whether this concept is appropriate,[51] the cases together propose that if the police use a surveillance device to obtain information they would not otherwise have been able to obtain lawfully, they violate the Fourth Amendment.[52]

43. *Id.* at 708.

44. *Id.*

45. *Id.* at 708–10. Over the course of four months, agents followed the beeper's signal from the defendant's home to his father's residence, two separate storage facilities, a codefendant's residence, and finally to the house rented by the conspirators. *Id.*

46. *Id.* at 713.

47. *Id.* at 714.

48. *Id.* at 715.

49. *Compare id.* at 714, *with* United States v. Knotts, 460 U.S. 276, 281–82 (1983).

50. *See Karo*, 468 U.S. at 732 (Stevens, J., concurring in part, dissenting in part) ("[The beeper] revealed only the route of a trip through areas open to the public, something that was hardly concealed from public view."); *see also* Katz v. United States, 389 U.S. 347, 351 n.9 (1967) (noting that the Court "has occasionally described its conclusions in terms of 'constitutionally protected areas'").

51. *See Katz*, 389 U.S. at 351 n.9 ("We have never suggested that this concept [of 'constitutionally protected areas'] can serve as a talismanic solution to every Fourth Amendment problem.").

52. *See Karo*, 468 U.S. at 716 ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.").

One of the most interesting technologically oriented Fourth Amendment cases is *Kyllo v. United States*.[53] Government agents used a thermal imaging device to scan Kyllo's house for signs of a marijuana-growing operation.[54] Using the thermal imaging information and other evidence, the agents obtained a warrant to search Kyllo's home, where they found marijuana growing.[55] Justice Scalia, writing for the majority, astutely noted that technological advances have changed the contours of Fourth Amendment privacy rights.[56] Nevertheless, some "minimal expectation of privacy" must still exist; to hold otherwise "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[57] The Court held: "[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use."[58]

Perhaps the greatest point of contention surrounding this case involves Scalia's phrase "general public use."[59] On its face, this test seems useful. A well-informed judge should usually be able to determine whether a device used by the police is also available to the public. But Justice Stevens, in his dissenting opinion in *Kyllo*, was quick to criticize this rule, calling it "at once too broad and too narrow."[60] As a device becomes easier to acquire and comes into general public use, any Fourth Amendment protection against the use of that device erodes, thus increasing the "threat to privacy" the device poses.[61]

Stevens further argued that the phrase "sense-enhancing technology" is too broad because it may encompass far too many things.[62] Additionally, the fact that the majority's rule applies to "any information regarding the

53. Kyllo v. United States, 533 U.S. 27 (2001).
54. *Id.* at 29–30.
55. *Id.* at 30.
56. *Id.* at 33–34.
57. *Id.* at 34.
58. *Id.* (citation omitted) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).
59. *Id.*
60. *Id.* at 47 (Stevens, J., dissenting).
61. *Id.*
62. *Id.* at 47–48. Stevens noted as an example that, under the majority's rule, using hypothetical "mechanical substitutes" for drug-sniffing dogs, which themselves do not constitute a Fourth Amendment search, would be unconstitutional. *Id.*

interior of the home" makes it too broad, in that it may include outside "information . . . that could lead to (however many) inferences 'regarding' what might be inside."[63] This part of the rule is also too narrow in that there are private places other than the home that surveillance equipment might access.[64]

B. *Branching Outward: More Recent Legal Developments*

In the years since *Kyllo*, some lower federal courts have also been active in deciding cases in this vein. Some of these newer cases have applied doctrine from one or more of the cases discussed in Part II.A,[65] while others have applied different rules,[66] depending on the situation presented in each case.

In *United States v. Forrester*, the Ninth Circuit was presented with an issue of first impression.[67] While investigating the defendant's ecstasy-manufacturing operation, federal agents installed—on the defendant's internet account—"a pen register analogue known as a mirror port," designed to enable the government to learn the senders and recipients of e-mails, IP addresses of visited websites, and volume of data sent to or from the account.[68] In its analysis, the Ninth Circuit applied the reasoning of *Smith*, noting the following similarities between the two cases: (1) use of a third-party intermediary to communicate; (2) presumption of common knowledge that certain information (in this case, e-mail and IP addresses) will be used by the service provider to complete the communication link; and (3) voluntary disclosure of that information to the service provider.[69] The court even contended that the government surveillance employed in this case was "conceptually indistinguishable from government surveillance

63. *Id.* at 48.

64. *Id.* at 48–49.

65. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that the use of computer surveillance revealing "the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account" was "constitutionally indistinguishable" from the pen register used in *Smith*).

66. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012) (holding that the search-incident-to-arrest doctrine allows officers to access data on an arrestee's cell phone, particularly the cell phone's number, without a warrant); *see also infra* Part III (discussing innovative approaches to Fourth Amendment cases involving technology used by courts).

67. *Forrester*, 512 F.3d at 510.

68. *Id.* at 505.

69. *Id.* at 510.

of physical mail," in that it was no different than examining "whatever information people put on the outside of mail."[70] As with "snail mail," the addresses of the sender and recipient of the e-mail are voluntarily conveyed to the carrier.[71] For these reasons, the government's surveillance of the defendants in this case was not a search.[72]

The rule is somewhat different when applied to the contents of e-mails. In *United States v. Warshak*, the Government, acting without a warrant, seized approximately 27,000 of Warshak's e-mails as part of a large fraud investigation.[73] The Sixth Circuit held that the Government violated Warshak's Fourth Amendment rights when it compelled his Internet service provider (ISP) to reveal the contents of the e-mails.[74] Pursuant to a provision of the Stored Communications Act (SCA), the Government first asked NuVox—Warshak's ISP—to preserve copies of all e-mails Warshak sent and received.[75] Using another SCA provision, the Government obtained a subpoena ordering NuVox to turn over the e-mails it had preserved.[76] The Government also obtained a court order requiring NuVox to turn over all of Warshak's other e-mails.[77]

The Sixth Circuit applied the two-pronged *Katz* test, inquiring into whether Warshak "manifested a subjective expectation of privacy" that "society [is] willing to recognize . . . as reasonable."[78] Warshak clearly met the subjective prong because many of the e-mails contained "sensitive and sometimes damning" information, and as the court pointed out, "people seldom unfurl their dirty laundry in plain view."[79] The court approached the objective prong seriously, noting that e-mail has become an increasingly important form of communication in recent years.[80] The court

70. *Id.* at 511.
71. *Id.*
72. *Id.*
73. United States v. Warshak, 631 F.3d 266, 274, 282–83 (6th Cir. 2010).
74. *Id.* at 282.
75. *Id.* at 282–83; *see also* Stored Communications Act, 18 U.S.C. § 2703(f) (2012).
76. *Warshak*, 631 F.3d at 283; *see also* 18 U.S.C. § 2703(b) (authorizing the government to subpoena electronic communications).
77. *Warshak*, 631 F.3d at 283; *see also* 18 U.S.C. § 2703(d) (authorizing the government to obtain ex parte court orders to reveal additional electronic communications).
78. *Warshak*, 631 F.3d at 284 (quoting California v. Ciraolo, 476 U.S. 207, 211 (1986)) (internal quotation mark omitted).
79. *Id.*
80. *Id.*

also emphasized the importance of keeping the Fourth Amendment in line with technological advancements, "or its guarantees will wither and perish."[81] Noting the similarities of e-mail to "traditional forms of communication," such as phone calls and letters, the court decided that it would not make sense for the Fourth Amendment to protect e-mail any less than it protects other communications.[82] Because the ISP is a necessary intermediary for e-mail communication, the court reasoned, it is "the functional equivalent of a post office or a telephone company."[83] Because the government violates the Fourth Amendment when it seizes a letter or surreptitiously records a phone conversation without a warrant, a violation also occurs when the government forces an ISP to turn over the contents of a user's e-mails.[84] The government therefore violated Warshak's Fourth Amendment rights, and the court held the SCA unconstitutional insofar as it "purports to permit the government to obtain such emails warrantlessly."[85]

Forrester and *Warshak* are perhaps comforting examples of straightforward application of precedent in a Fourth Amendment case. From a judicial standpoint, it is fortunate that the technology used in *Forrester* so closely matched the *Smith* pen register, especially given the fact that the case presented an issue of first impression for the Ninth Circuit.[86] The Sixth Circuit, meanwhile, had no trouble analogizing e-mail to "traditional forms of communication."[87] However, analogical reasoning in Fourth Amendment cases involving law enforcement use of new technology is, regrettably, not always such a simple exercise.

1. *The New Era:* Jones *and What It Changed*

In *United States v. Jones*, the police acted outside the scope of a warrant they had obtained and attached a GPS tracking device to Jones's vehicle.[88] The police tracked the vehicle's movements for four weeks and

81. *Id.* at 285.

82. *Id.* at 285–86.

83. *Id.* at 286.

84. *Id.*; *see also* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (holding that a warrantless search of a sealed package violates the Fourth Amendment); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the Government's eavesdropping on a telephone conversation constituted a Fourth Amendment search and seizure).

85. *Warshak*, 631 F.3d at 288.

86. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

87. *See Warshak*, 631 F.3d at 285–86.

88. United States v. Jones, 132 S. Ct. 945, 948 (2012). The use of the GPS

compiled reams of location data.[89] The Supreme Court held that this long-term GPS tracking was a search.[90] The Court focused mostly on a property-rights analysis, noting that the language of the Fourth Amendment is couched in terms of property.[91] *Katz*, the Court insisted, did not "repudiate th[e] understanding" that the Fourth Amendment guards against government trespass on certain constitutionally protected areas.[92] Applying this principle, the Court concluded that the installation and use of the GPS tracker on Jones's vehicle constituted a physical intrusion on private property to obtain information.[93]

Because it relied so much on intrusion of property rights to reach its conclusion, *Jones* resurrected an area of Fourth Amendment jurisprudence to a prominence that it had not enjoyed since before *Katz*.[94] *Jones* should allow defense attorneys litigating similar cases to use a new (and simultaneously old) line of attack in arguing suppression motions.[95] Attorneys could potentially employ the physical intrusion argument in many situations, although it is unclear what these situations might be.

III. OTHER WAYS OF VIEWING THE INTERACTION OF TECHNOLOGY AND THE FOURTH AMENDMENT

Courts have taken sophisticated—and sometimes innovative—approaches to Fourth Amendment cases involving technology.[96] This Part discusses other possible approaches from other areas of Fourth

tracking device was outside the scope of the warrant for two reasons: (1) it was attached one day outside of the 10 day window, and (2) it was attached in Maryland instead of in the District of Columbia. *Id.*

89. *Id.*

90. *Id.* at 949.

91. *Id.*

92. *Id.* at 950.

93. *Id.* at 949.

94. *See id.* at 950–51 (noting that, although *Katz* and its progeny "have deviated from that exclusively property-based approach," the holding in "*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment'" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring))); *see also* Katz v. United States, 389 U.S 347, 352–53 (1967) (holding that because the Fourth Amendment protects both people and their property, the unconstitutionality of a search or seizure is not solely dependent upon a physical intrusion).

95. *See Jones*, 132 S. Ct. at 949.

96. *See infra* Part III.A–C.

Amendment jurisprudence and ideas from commentators.

A. *How the Technology in Question Works*

What a certain device can do is often a central question in Fourth Amendment case law.[97] In *United States v. Vela*, a border patrol agent, while tracking Vela's vehicle, used night vision goggles to see inside it.[98] After the agent stopped Vela, he discovered she was smuggling illegal aliens.[99]

The district court distinguished this case from *Kyllo* in two ways.[100] First, Vela was in her car on a public road, not in her private residence, meaning she had a somewhat reduced expectation of privacy.[101] Second, the technology the agent used in *Vela* was significantly different from the thermal imaging device used in *Kyllo*.[102] Night vision goggles "merely amplify light,"[103] and they are widely available for sale to the public in stores and on the Internet.[104] Because of the widespread availability of night vision goggles and their technological limitations, the court held that the agent's use of the goggles to see inside Vela's vehicle was not a search.[105]

B. *The Importance of Context*

The context in which a search occurs, regardless of whether monitoring of electronic communications is involved, is significant.[106] Many

97. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 35–36 (2001) (addressing the dissent's argument about "off-the-wall" versus "through-the-wall" thermal imaging surveillance and concluding that "[w]hile the [off-the-wall] technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development").

98. United States v. Vela, 486 F. Supp. 2d 587, 589 (W.D. Tex. 2005).

99. *Id.*

100. *Id.* at 589–90.

101. *Id.* at 589.

102. *Id.* at 590.

103. *Id.* The court explained that "[t]he goggles merely amplify ambient light to see something that is already exposed to public view. This type of technology is no more 'intrusive' than binoculars or flashlights." *Id.* Thermal imaging devices, on the other hand, are capable of penetrating walls and detecting things that are not readily visible, "provid[ing] information that would otherwise require physical intrusion." *Id.*; *see also* Kyllo v. United States, 533 U.S. 27, 34–36 (2001).

104. *Vela*, 486 F. Supp. 2d at 590.

105. *Id.*

106. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion)

employers monitor some or all of the electronic communications their employees send and receive on company-owned devices, although employees still have some rights that courts are prepared to recognize in this arena.[107]

A helpful case for analyzing and discussing employees' expectations of privacy in their electronic communications, at least when the employer in question is a government entity, is *City of Ontario v. Quon*.[108] Quon was a SWAT police sergeant for the Ontario Police Department (OPD) in Ontario, California.[109] The City of Ontario bought pagers that could send and receive text messages for the SWAT team members "in order to help the SWAT Team mobilize and respond to emergency situations."[110] Pursuant to a contract between the city and a wireless service provider, each pager could only send or receive a certain number of characters in a given month.[111] Any excess characters sent or received would trigger a surcharge.[112] The city also had a policy regarding its internal communications network, whereby it "reserve[d] the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have *no expectation of privacy or confidentiality* when using these resources."[113] Quon was told this policy would apply to text messages sent and received via the new pagers.[114] After Quon went over his monthly character allotment several times, OPD leadership obtained transcripts of Quon's messages from the wireless service provider.[115] The chief of OPD wanted to determine whether the overages were the result of personal or work-related messages.[116] The vast majority of Quon's

(noting that, in the context of government offices, many people, including the public, may have access to a given employee's office, lowering the employee's reasonable expectation of privacy).

107. *See* Dionne Searcey, *Some Courts Raise Bar on Reading Employee Email*, WALL ST. J. (Nov. 24, 2009), http://online.wsj.com/article/SB125859862658454923.html (discussing, *inter alia*, the recent trend in employee-privacy litigation that "courts are increasingly taking into account whether employers have explicitly described" their e-mail monitoring policy to their employees).

108. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

109. *Id.* at 2624.

110. *Id.* at 2625.

111. *Id.*

112. *Id.*

113. *Id.* (emphasis added) (internal quotation marks omitted).

114. *Id.*

115. *Id.* at 2625–26.

116. *Id.* at 2626.

messages sent or received during work hours turned out to be not work related.[117] After an internal affairs investigation that led to disciplinary measures against him, Quon sued the city and others, alleging a violation of his Fourth Amendment rights.[118]

The Supreme Court approached this case with caution and framed the issue narrowly.[119] The Court warned about the risks involved in cases like this; unintended detrimental consequences could result from an overly broad ruling about "emerging technology before its role in society has become clear."[120] The Court also pointed out that changes in "the dynamics of communication" result from social norms as well as technological development.[121] There have also been recent developments in this area of law, with some states passing statutes that require employers to inform employees of the monitoring of electronic communications.[122] However, because the city had a legitimate reason to conduct the search, and because the search was not "excessively intrusive," the Court held that the search was reasonable and did not violate Quon's Fourth Amendment rights.[123]

C. *Social Understanding: The Unwritten Code of Technology*

Another way of looking at how technology interacts with the Fourth Amendment is to think about the "social understanding" surrounding the technology at issue.[124] This may lead to a different solution than the "inner workings" analysis because, in some circumstances, for example, people "still consider their communications over wireless networks to be private in nature."[125] A creative defense attorney could certainly argue that there is

117. *Id.*

118. *Id.*

119. *See id.* at 2629 ("The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer.").

120. *Id.*

121. *Id.*

122. *Id.* at 2630.

123. *Id.* at 2633.

124. *See* Orin Kerr, *Do Users of Wi-Fi Networks Have Fourth Amendment Rights Against Government Interception?*, VOLOKH CONSPIRACY (Sept. 24, 2012), http://www.volokh.com/2012/09/24/fourth-amendment-rights-for-users-of-wi-fi-networ ks-both-encrypted-and-unencrypted/ (noting that, in the context of wireless networks, the reasonableness of an individual's expectation of privacy can greatly differ when viewed from the social understanding of the technology—rather than from the capabilities of technology itself).

125. *Id.*

an objectively reasonable expectation of privacy in certain kinds of communications, even though such communications are broadcast over unsecured wireless networks. Unfortunately, such an argument would likely be a losing one.

In *United States v. Stanley*, a federal district court ruled on the question of whether a user has a reasonable expectation of privacy in the use of an unsecured wireless signal.[126] Robert Erdely, head of the Pennsylvania State Police's computer crime unit, found a computer sharing many files, some of which he believed might contain child pornography, on a file-sharing network.[127] Erdely was able to confirm his suspicion using a law enforcement child pornography database.[128] Erdely then traced the computer's IP address via the file-sharing network.[129] Erdely obtained a court order telling the service provider to give him the identity and street address of the IP address's owner, a man named William Kozikowski.[130] After searching Kozikowski's home, Erdely did not find the subject computer.[131] However, the home did contain an unsecured (i.e. not password protected) wireless router.[132] After lengthy surveillance of the computers that accessed Kozikowski's router, Erdely traced the offending file-sharing activity to the subject computer's IP address.[133] Erdely then used a program called Moocherhunter to trace the physical location of the subject computer.[134] After determining that the signal Moocherhunter detected was emanating from Richard Stanley's apartment, Erdely obtained a search warrant for that apartment.[135]

The court in this case specifically described the inner workings of the technology in question.[136] Ultimately, the court considered the Moocherhunter software to be similar to the pen register in *Smith*, in that

126. United States v. Stanley, Criminal No. 11-272, 2012 WL 5512987, at *11 (W.D. Pa. Nov. 14, 2012).

127. *Id.* at *1–2.

128. *Id.* at *2.

129. *Id.*

130. *Id.* at *2–3.

131. *Id.* at *3.

132. *Id.*

133. *See id.* at *4–6.

134. *Id.* at *6.

135. *Id.* at *7–8.

136. *See id.* at *3–4 (explaining how wireless routers work, how computers access such routers, and the difference between public and private IP addresses). The court also gave a detailed account of what Moocherhunter does. *Id.* at *6–7.

Moocherhunter only showed the existence of the communications, not their contents.[137] Moreover, Stanley voluntarily accessed Kozikowski's wireless router without Kozikowski's permission, meaning he assumed the risk that his communications might become known to the police.[138] Stanley, like Smith, voluntarily conveyed information to a third party; Smith conveyed the numbers he dialed to the phone company, while Stanley conveyed his IP address to Kozikowski's router.[139] For these reasons, Stanley did not have a reasonable expectation of privacy in the signal he used to connect to the Internet via Kozikowski's wireless router.[140] One commentator agreed with this case's application of *Smith*, adding that it presents "a pretty interesting set of facts."[141]

D. *Rethinking Core Principles*

Judges and practitioners may need to question the core principles of the Fourth Amendment and the attendant case law in order to solve the creeping technology problem. The primary concern is that privacy rights erode as technology improves.[142]

Examining the first principles of Fourth Amendment jurisprudence requires careful parsing of the *Katz* phrase "reasonable expectation of privacy."[143] "The very word[] 'reasonable' . . . [is] tightly linked to 'ratio'—which is to say, to relative magnitude or balance."[144] The implicit object of many cases interpreting the Fourth Amendment, then, is to balance the need for privacy against the need for security.[145] This is problematic because it implies a zero-sum continuum: to increase privacy, one must

137. *Id.* at *12.

138. *Id.*

139. *Id.*; *see* Smith v. Maryland, 442 U.S. 735, 744 (1979).

140. *Stanley*, 2012 WL 5512987, at *12, *14.

141. Orin Kerr, United States v. Stanley *and the Fourth Amendment Implications of Using "Moocherhunter" to Locate the User of an Unsecured Wireless Network*, VOLOKH CONSPIRACY (Nov. 19, 2012), http://www.volokh.com/2012/11/19/united-states-v-stanley-and-the-fourth-amendment-implications-of-using-moocherhunter-to-locate-the-user-of-an-unsecured-wireless-network/.

142. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

143. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

144. Julian Sanchez, *The Trouble with "Balance" Metaphors*, JULIANSANCHEZ (Feb. 4, 2011), http://www.juliansanchez.com/2011/02/04/the-trouble-with-balance-metaphors/.

145. *See id.*

sacrifice an equal measure of security, and vice versa.[146] This construct also implies that equilibrium, or balance, is the goal, and that anything other than perfect balance is undesirable.[147] Perhaps the core problem with the idea of a zero-sum continuum is that it "leads people to view [privacy and security] as *always* in conflict," even though this is not necessarily true.[148]

Another problem with the idea of balance in this realm of law is that it "reduc[es] diverse objects . . . to a single shared dimension."[149] The problem is that, unlike an actual scale, jurists and practitioners do not understand what the standard of comparison is between privacy and security, or whichever two values are under consideration.[150] To make matters worse, "privacy" and "security" are not monolithic concepts; they are complex.[151] As writer Julian Sanchez wonders, "[I]s it really especially illuminating to treat every proposed security measure as though its consequences can be reduced to quantity subtracted from an undifferentiated lump of privacy stuff, and a quantity added to a blob called security?"[152] The rhetorical question illustrates Sanchez's point: Balancing tests are an analytical shortcut courts use to oversimplify—to a worrisome degree—the problems with which they are presented.[153]

In a similar vein with Sanchez, Professor Orin Kerr has called the "patchwork" of rules used in Fourth Amendment case law "a theoretical embarrassment to scholars and judges alike."[154] However, Kerr attempts to explain the Supreme Court's jurisprudential methodology in many Fourth Amendment cases, calling it "equilibrium-adjustment."[155] In response to changing technology, social norms, and other key facts, courts adjust the balance between privacy and security to conform to the balance that

146. *Id.*

147. *Id.*

148. *Id.*

149. *Id.* Sanchez illustrates: "You might have items as varied as toasters and giraffes on the opposing plates of the scale, but all the scale cares about—or all we care about when we employ it—is that they both have weight and mass." *Id.*

150. *See id.*

151. *Id. See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 480–82 (2006) (arguing that a clearer, more nuanced understanding of the concept of privacy is necessary to rectify privacy violations).

152. Sanchez, *supra* note 144.

153. *See id.*

154. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

155. *Id.*

previously prevailed.[156] Equilibrium-adjustment can occur in several different scenarios, including when "the government uses a surveillance device to obtain information that previously would have been unobtainable or less easily obtained."[157] By adjusting the legal rules, the courts thereby preserve the status quo "equilibrium" of Fourth Amendment protection.[158] However, because technology changes so rapidly, it is often difficult for courts to react in a timely manner.[159] Moreover, when judges engage in equilibrium-adjustment, they act to preserve order, with the idea that "[i]nsufficient police power will leave the police unable to enforce the law."[160] Equilibrium-adjustment goes hand-in-hand with traditional common law analogical reasoning from existing case law, although equilibrium-adjustment is more oriented than common law reasoning toward the status quo.[161] Kerr cites *Kyllo* as an illustrative example of equilibrium-adjustment in action.[162]

IV. THE UBIQUITY OF TECHNOLOGY IN LAW ENFORCEMENT AND ITS EFFECT ON PRIVACY

A common theme in many of the cases discussed elsewhere in this Note is the technology used by law enforcement agencies.[163] However, there are many other devices in the modern police officer's toolbox. This Part only covers a small number of high-profile technological developments law enforcement agencies have recently added to their arsenals. Unfortunately, any discussion of the potential Fourth Amendment consequences of these developments amounts to little more than theoretical reasoning based on analogies drawn from existing case law.

A. *Mass Data Collection and Integrated Surveillance Systems*

The modern American surveillance state has been a subject of some contention lately. The current debate centers on the National Security

156. *Id.* at 482.
157. *Id.* at 489.
158. *See id.* at 480.
159. *See id.* at 485 ("[T]he facts of criminal investigations, and therefore the facts that the Fourth Amendment regulates, are constantly evolving in response to technological and social change.").
160. *Id.* at 488.
161. *Id.* at 492–93.
162. *Id.* at 496–99.
163. *See supra* Parts II, III.

Agency's collection of massive amounts of communications data under programs such as Boundless Informant and Prism.[164] The former program collects "records of communications," or metadata, on electronic communications networks around the world.[165] Prism, on the other hand, "allows officials to collect material including search history, the content of emails, file transfers and live chats" from "the systems of Google, Facebook, Apple, and other US internet giants."[166] It is not difficult to see why it may be problematic that intelligence and law enforcement agencies are employing such sweeping—and arguably invasive—surveillance protocols. Such programs have developed in response to terrorism and other threats to national security.[167] However, sophisticated and far-reaching law enforcement surveillance does not only prevail at the national level; it has permeated state and local law enforcement agencies as well.

When discussing trends in local law enforcement, it is perhaps most instructive to look at the New York Police Department (NYPD), which far outclasses any other American police force in manpower and resources.[168] New York Mayor Michael Bloomberg once bragged that the NYPD is his own personal army.[169] The NYPD also has the Domain Awareness System

164. *See* Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [hereinafter *Boundless Informant*]; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [hereinafter *Prism*].

165. Greenwald & MacAskill, *Boundless Informant*, *supra* note 164.

166. Greenwald & MacAskill, *Prism*, *supra* note 164.

167. *See id.* ("Prism was introduced to overcome what the NSA regarded as shortcomings of [Foreign Intelligence Surveillance Act] warrants in tracking suspected foreign terrorists.").

168. *See* Tana Ganeva & Laura Gottesdiener, *9 Frightening Things about America's Biggest Police Force*, ALTERNET (Sept. 27, 2012), http://www.alternet.org/civil-liberties/9-frightening-things-about-americas-biggest-police-force? (noting that the NYPD has more employees than the FBI and a proposed budget of about 15 percent of the City of New York's entire budget). *See generally* RADLEY BALKO, RISE OF THE WARRIOR COP: THE MILITARIZATION OF AMERICA'S POLICE FORCES (2013) (discussing the escalation of technology, equipment, tactics, and methods in modern law enforcement in the United States with a focus on, among other things, the war on drugs and the origins of the SWAT unit).

169. *'I Have My Own Army in the NYPD—The Seventh Largest Army in the World': Bloomberg's Bizarre Boast About City's Police Force*, MAIL ONLINE, (Dec. 1, 2011), http://www.dailymail.co.uk/news/article-2068428/Bloomberg-I-army-NYPD-State-Department-New-York-City.html. Though Bloomberg was almost certainly joking,

(DAS), a new surveillance system that "will collect and archive data from thousands of . . . [closed-circuit television] cameras in New York City, integrate license plate readers, and instantly compare data from multiple non-NYPD intelligence databases."[170] Most of the cameras are in "strategic transportation points like bridges and tunnels," and the system also uses radiation detectors.[171] Because so many of these cameras are on public roads and in other public areas, it is doubtful that courts would object to DAS, far-reaching though it may be.

B. *Unmanned Aerial Vehicles*

In recent years, much has been made of the use of unmanned aerial vehicles, commonly known as drones, in law enforcement activities.[172] Drones are available in many different varieties.[173] These aircraft can easily carry powerful surveillance equipment.[174] Many local and federal law enforcement agencies are beginning to test drones with plans to expand their use of these aircraft.[175] The Orwellian implications of drone-based surveillance are obvious.[176] The government could easily use and abuse

many police departments around the country—with some financial help from the federal government—have been militarizing their equipment and methods to the point of alarming excess. For an in-depth discussion of this trend, see Andrew Becker & G.W. Schulz, *Local Cops Ready for War with Homeland Security-Funded Military Weapons*, DAILY BEAST (Dec. 21, 2011), http://www.thedailybeast.com/articles/2011/12/20/local-cops-ready-for-war-with-homeland-security-funded-military-weapons.html.

170. Neal Ungerleider, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" with Real-Time CCTV, License Plate Monitoring*, FAST COMPANY (Aug. 8, 2012), http://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

171. *Id.*

172. *See* Walter Hickey, *These Police Surveillance Drones Could Be Watching You Right Now*, BUS. INSIDER (July 10, 2012), http://www.businessinsider.com/us-police-drones-2012-7?op=1 (discussing several different types of surveillance drones currently being used by a number of police departments in major American and Canadian cities, including Miami, Los Angeles, Seattle, and Saskatoon, Saskatchewan).

173. *See* AM. CIVIL LIBERTIES UNION, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 2–4 (2011), *available at* http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf (identifying several general types of drones used by the U.S. military and various American law enforcement agencies).

174. *See id.* at 4–6 (outlining different types of surveillance devices and technologies drones can carry, including see-through imaging and facial recognition).

175. *See id.* at 6–8.

176. *See id.* at 13 ("With drone technology holding so much potential to

these drones to spy on people almost anywhere; indeed, the American Civil Liberties Union (ACLU) is concerned that the mere possibility of such spying might have a "chilling effect" on people's behavior.[177] Although it has not ruled on the use of drones, the Supreme Court has consistently allowed warrantless surveillance from manned aircraft.[178] The ACLU argues that drones, with their sophisticated surveillance devices, are more intrusive on privacy than reconnaissance flights in manned aircraft.[179] The ACLU relies in part on the Supreme Court's holding in *Kyllo* to establish this point.[180]

The ACLU recommends that unmanned aerial vehicles (UAVs) should only be used under specific circumstances.[181] Criminal investigators should only deploy a drone when "there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the drone will intrude upon reasonable expectations of privacy, whe[n] the government has obtained a warrant based on probable cause."[182]

The ACLU also advocates for considerable transparency in the use of drones.[183] It recommends that "policies and procedures for the use of aerial surveillance technologies" should be a matter of public record, although it acknowledges that information pertinent to specific ongoing investigations can and should be kept confidential.[184] The ACLU also proposes that the use of UAVs be meticulously analyzed and tracked in order to inform citizens about whether UAVs are serving the public properly.[185] The ACLU believes that the use of UAVs should be "democratically decided

increase routine surveillance in American life, one key question is the extent to which our laws will protect us.").

177. *Id.* at 11.

178. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that officers' visual surveillance of defendant's fenced-in backyard from a manned plane flying overhead in "public navigable airspace" did not violate defendant's Fourth Amendment rights); *see also* AM. CIVIL LIBERTIES UNION, *supra* note 173, at 13–14.

179. AM. CIVIL LIBERTIES UNION, *supra* note 173, at 14.

180. *Id.*; *see also* Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) ("[S]urveillance of private property by using highly sophisticated surveillance equipment not generally available to the public . . . might be constitutionally proscribed absent a warrant.").

181. AM. CIVIL LIBERTIES UNION, *supra* note 173, at 15–16.

182. *Id.* at 15.

183. *See id.* at 16.

184. *Id.*

185. *Id.*

based on open information," but it does not elaborate on what it means by this.[186]

On the other hand, concerns about law enforcement use of unarmed surveillance drones may be overblown. The police department for Monroe, North Carolina, recently purchased such a drone.[187] This particular model of drone, known as the Maveric, comes equipped with a GPS and is radio controlled.[188] The head of Condor Aerial, the company that designed and built the Maveric drone, pointed out that the drone's average flight time was approximately 60 to 90 minutes, contrary to the constant and pervasive surveillance people often fear when they think of drones.[189] It is also worth noting that the Maveric model has been publicly available for a decade and that it is not an imposing machine; it is small enough that a man can hold it in one hand.[190] One commentator has called it "a radio controlled toy airplane with a fancy camera."[191]

A drone used merely for "eyes in the sky" visual surveillance would likely be no less constitutionally permissible than visual surveillance from a manned aircraft, assuming that the drone is passing through public airspace.[192] However, the ACLU's concerns about transparency in the use of drones are well-founded, albeit somewhat incompletely stated.[193] The ACLU is not alone; Senator Rand Paul has also called for more governmental transparency regarding the use of drones.[194] One resident of

186. *Id.*

187. Carolyn Steeves, *Police Get an 'Eye in the Sky'*, MONROE ENQUIRER-J. (Mar. 5, 2013), http://www.enquirerjournal.com/news/local/x1942451247/Police-get-an-eye-in-the-sky; *see also* Bob Cesca, *The Most Terrifying Drone Ever! Run Away!*, DAILY BANTER (Mar. 13, 2013), http://thedailybanter.com/2013/03/the-most-terrifying-drone-ever-run-away/ (characterizing the drone being used by the Monroe Police Department as little more than a cheaper alternative to a manned surveillance aircraft, such as a helicopter).

188. Steeves, *supra* note 187.

189. *Id.*

190. *See* Cesca, *supra* note 187.

191. *Id.*

192. *Cf.* California v. Ciraolo, 476 U.S. 207, 213–14 (1986). *But see* AM. CIVIL LIBERTIES UNION, *supra* note 173, at 13 ("The Supreme Court has never taken a position on whether the Fourth Amendment places limits on government use of UAV surveillance.").

193. *See* AM. CIVIL LIBERTIES UNION, *supra* note 173, at 16.

194. *See* Ed O'Keefe & Aaron Blake, *Paul's Filibuster in Opposition to Brennan, Drone Policy Ends After Nearly 13 Hours*, WASH. POST POL. (Mar. 6, 2013), http://www.washingtonpost.com/politics/rand-paul-conducts-filibuster-in-opposition-to-john-brennan-obamas-drone-policy/2013/03/06/1367b1b4-868c-11e2-9d71-f0feafdd1394

a small Colorado town has proposed an ordinance to the town's board of trustees that would permit shooting drones out of the sky with a twelve-gauge shotgun.[195] Law enforcement agencies using unarmed drones for surveillance could stand to be more forthcoming about how they deploy their drones, although it would obviously not be in the public interest to force the police to disclose too much information about investigations.

V. CONCLUSION

Technology is ever marching forward, such that the definition of "general public use" from *Kyllo*[196] could change completely between now and next year. Applicable case law is also changing, but it remains to be seen whether Fourth Amendment jurisprudence is as adaptable as it needs to be to protect against the dangers that high-tech law enforcement might pose. The *Jones* case may have illuminated this entire area of law, or it may have merely reshuffled the deck.[197] Only time will tell.

In any event, judges' and practitioners' conceptions of "privacy" as protected by the Fourth Amendment may need to evolve to meet the trend of continual technological improvement.[198] Legal professionals and judicial officials—and the American people—must ensure that law enforcement agencies do not abuse their modern tools in a way that circumvents or undermines the Fourth Amendment's guarantees. It is up to these decision makers to ensure that the Fourth Amendment does not weaken or fail.

*Blake Stubbs**

_story.html (discussing Senator Paul's filibuster against the nomination of John Brennan for the position of CIA Director, in which Paul "said he was 'alarmed' by a lack of definition for who can be targeted by drone strikes"). It should be noted, however, that Paul was particularly discussing the use of armed drones for targeted killings, not the use of unarmed drones for aerial surveillance. *See id.*

195. Conor Friedersdorf, *Local Anti-Drone Activism Begins: 'If They Fly in Town, We Will Shoot Them Down,'* ATLANTIC (July 30, 2013), http://www.theatlantic.com/politics/archive/2013/07/local-anti-drone-activism-begins-if-they-fly-in-town-we-will-shoot-them-down/278198/.

196. Kyllo v. United States, 533 U.S. 27, 34 (2001).

197. *See* discussion *supra* Part II.B.

198. *See* discussion *supra* Part III.D.

* B.A. Washington University in St. Louis, 2011; J.D. Candidate, Drake University Law School, 2014.