THE FOURTH AMENDMENT AND TECHNOLOGICALLY BASED SURVEILLANCE

Russell L. Weaver[*]

I. INTRODUCTION

Over the centuries, technological advances have unalterably affected society. For example, in the fifteenth century, Johannes Gutenberg's invention of the printing press revolutionized communication.[1] Gutenberg's invention is credited with leading to the Renaissance, the Scientific Revolution, and the Protestant Reformation.[2] As transformative as the printing press might have been, modern communications technologies have made the Gutenberg press seem quaint and antiquated. The Internet and devices like "smart phones" have enabled ordinary people to engage in mass communication and have transformed the dynamics of the political process.[3]

Technological advances have not been limited to communications but instead have also transformed police surveillance technologies.[4] In the early twentieth century, the police used devices such as "detectaphones,"[5] wiretapping,[6] and parabolic microphones.[7] As the century progressed, the technologies available to police investigators steadily improved, and the

---

* Professor of Law and Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law.

1. *See* RUSSELL L. WEAVER, FROM GUTENBERG TO THE INTERNET: FREE SPEECH, ADVANCING TECHNOLOGY, AND THE IMPLICATIONS FOR DEMOCRACY 5–6 (2013).

2. *See* Rogelio Lasso, *From the Paper Chase to the Digital Chase: Technology and the Challenge of Teaching 21st Century Law Students*, 43 SANTA CLARA L. REV. 1, 4–5 (2002).

3. *See* WEAVER, *supra* note 1.

4. *See* Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1134–36 (2011).

5. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 131 (1942) (describing a detectaphone), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

6. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 455 (1928), *overruled in part by Katz*, 389 U.S. 347.

7. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 508 (1961) (describing a parabolic microphone).

police were able to use helicopters,[8] global positioning systems,[9] and devices that allow the police to hear through walls,[10] as well as to peer through them.[11]

While technological advances have produced societal benefits (such as increased communication capacity and more effective police investigations), they have also produced adverse consequences for personal privacy.[12] Beginning in the early part of the twentieth century, individual U.S. Supreme Court Justices began raising concerns regarding the potential impact of advancing technologies on individual privacy.[13] For example, in *Olmstead v. United States*, a dissenting Justice Brandeis expressed concern that the "progress of science . . . is not likely to stop with wire tapping," and may someday allow the government, "without removing papers from secret drawers," to "expose to a jury the most intimate occurrences of the home."[14] Justice Brandeis argued for the need to protect the "indefeasible right of personal security, personal liberty and private property."[15] In *Goldman v. United States*, a dissenting Justice Murphy relied on Justices Brandeis and Warren's seminal article on privacy to argue that the Fourth Amendment should be broadly interpreted to protect "the individual against unwarranted intrusions by others into his private affairs," and to provide greater protection for individual privacy.[16]

Both Justice Brandeis and Justice Murphy were prescient.[17] Indeed, in 2013, Edward Snowden, a former employee for a contractor at the National Security Agency (NSA), shocked the nation when he stole and released thousands of classified documents, revealing that the NSA was operating a massive secret governmental cyber-surveillance operation.[18] Although U.S. citizens might have anticipated that the U.S. government was collecting information about alleged terrorists and criminals, few could have imagined the all-encompassing nature of the NSA surveillance program.[19] With a

---

8. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451–52 (1989) (holding that police observations made from a helicopter hovering at a legal altitude did not violate the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 214–15 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

9. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 285 (1983).

10. *See Goldman*, 316 U.S. at 131.

11. *See* Brad Heath, *New Police Radars Can 'See' Inside Homes*, USA TODAY (Jan. 20, 2015, 1:27 PM), http://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/.

12. *See infra* notes 20–22 and accompanying text.

13. *See, e.g.*, *Goldman*, 316 U.S. at 139 (Murphy, J., dissenting); Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

14. *Olmstead*, 277 U.S. at 474.

15. *Id.* at 474–75.

16. *Goldman*, 316 U.S. at 136 (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890)).

17. *See infra* text accompanying notes 48–52.

18. *See* Scott Shane, *No Morsel Too Minuscule for All-Consuming NSA*, N.Y. TIMES (Nov. 2, 2013), http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?_r=0; Doug Stanglin, *Report: Snowden Says NSA Can Tap E-mail, Facebook Chats*, USA TODAY (July 31, 2013, 11:49 AM), http://www.usatoday.com/story/news/nation/2013/07/31/edward-snowden-guardian-nsa-facebook-tap-email-documents/2602519/.

19. *See* Stanglin, *supra* note 18.

budget of $10.8 billion per year and 35,000 employees, the NSA systematically collected data about virtually everyone and everything, including millions of cell phone call records, emails, text messages, credit card purchase records, and information from social media networks.[20] In addition, the NSA had created a system (called MUSCULAR) that enabled it to easily access Yahoo and Google accounts.[21] The end result was that the NSA intercepted some 182 million communication records, including "to" and "from" email information, as well as text, audio, and video information.[22] As discussed more fully below, the U.S. Supreme Court's Fourth Amendment jurisprudence has not kept pace with advances in technology and has provided American citizens with very little protection against what can only be referred to as a technological onslaught.[23]

This Article does several things. First, it discusses the historical background of the U.S. Constitution, in particular the Bill of Rights, as well as the concerns and motivations that led to the adoption of the Fourth Amendment.[24] Second, it examines U.S. Supreme Court precedent applying the Fourth Amendment and suggests that this precedent has failed to provide Americans with adequate protection against governmental tracking and surveillance.[25] Finally, this Article suggests that there is some reason to be hopeful regarding the future of the Fourth Amendment and its ability to protect individuals against governmental tracking but expresses concern given the fact that the Court has generally failed to interpret the Fourth Amendment in an expansive manner.[26]

II. THE PHILOSOPHICAL UNDERPINNINGS OF THE FOURTH AMENDMENT

Adoption of the Fourth Amendment to the U.S. Constitution was motivated by abuses during the British colonial period.[27] British colonial

---

20. *See id.*; Peter Maass, *How Laura Poitras Helped Snowden Spill His Secrets*, N.Y. TIMES (Aug. 13, 2013), http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=all; Charlie Savage, *C.I.A. Is Said to Pay AT&T For Call Data*, N.Y. TIMES (Nov. 7, 2013), http://www.nytimes.com/2013/11/07/us/cia-is-said-to-pay-att-for-call-data.html.

21. *See* Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

22. *See* Martha Mendoza, *Reagan Order Led to NSA's Broader Spying on Internet*, USA TODAY (Nov. 21, 2013, 4:02 AM), http://usatoday30.usatoday.com/USCP/PNI/Business/2013-11-21-NSA-Taps-TechAAAWIRESBrd_ST_U.htm.

23. *See infra* Part III.

24. *See infra* Part II.

25. *See infra* Part III.

26. *See infra* Part IV.

27. *See* U.S. CONST. amend. IV; United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) ("The driving force behind the adoption of the [Fourth] Amendment . . . was widespread hostility among the former colonists to the issuance of writs of assistance. . . . [T]he purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government . . . .");

officials used writs of assistance that required "them to do no more than specify the object of a search" to "obtain a warrant [that] allow[ed] them to search any place where the goods might be found."[28] There was no limit as to place or duration.[29] "Colonial officials had also used 'general warrants' that required them only to specify an offense, and then left it to the discretion of executing officials to decide which persons should be arrested and which places should be searched."[30]

In adopting the Fourth Amendment, the founding generation sought to cabin the new government's authority to engage in searches and seizures and to limit the possibilities for abuse.[31] In general, the Fourth Amendment prohibited "unreasonable" searches and seizures.[32] Although the Amendment did not mandate the issuance of a search warrant as a precondition to a valid search, it did provide that "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."[33] Although the Fourth Amendment did not explicitly protect individual privacy, it did protect the security of people, as well as their houses, papers, and effects.[34]

III. THE LIMITS OF THE COURT'S FOURTH AMENDMENT JURISPRUDENCE

Although the Fourth Amendment has generally provided the citizenry with substantial protections against traditional searches and seizures, such as those conducted by British colonial officials,[35] it has not provided much protection against advancing technology.[36] The state of technology was far less advanced in the eighteenth century, and the founding generation was much more concerned about actual physical searches of persons and places than about technological intrusions.[37] As a result, the U.S. Supreme Court initially held that a search occurred only when the police actually searched a person or trespassed into a "constitutionally protected area."[38] Absent a

---

Boyd v. United States, 116 U.S. 616, 625 (1886) (discussing colonial backlash against the British writs of assistance and the invasions of privacy that accompanied them).

28. *See* Weaver, *supra* note 4, at 1131.
29. *See id.* at 1132.
30. *Id.*
31. *See Boyd*, 116 U.S. at 625.
32. *See* Weaver, *supra* note 4, at 1132.
33. U.S. CONST. amend. IV.
34. *See id.*
35. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 351 (2009); Kyllo v. United States, 533 U.S. 27, 40 (2001); Florida v. Royer, 460 U.S. 491, 504–08 (1983); Mapp v. Ohio, 367 U.S. 643, 660 (1961).
36. *See* Weaver, *supra* note 4, at 1155–58.
37. *See* Draper v. United States, 358 U.S. 307, 317–20 (1959) (Douglas, J., dissenting).
38. *See id.*; Silverman v. United States, 365 U.S. 505, 512 (1961).

trespassory intrusion, there was no search, and the Fourth Amendment was inapplicable.[39]

By the beginning of the twentieth century, as electricity came into widespread use and new technologies were invented that employed electricity, the Court began to confront situations in which the police or governmental officials aggressively used new technologies in police investigations.[40] In these early cases, the Court dealt with relatively crude technologies such as detectaphones,[41] "spike mikes,"[42] and wiretaps.[43]

Early decisions provided little protection against these new technologies. Except when the technology actually penetrated into a constitutionally protected area, such as a home, the Court refused to hold that the use of such technologies to spy on citizens constituted a "search" within the meaning of the Fourth Amendment.[44] As a result, the Court's approach provided little protection in situations in which the police used technology to spy on people without actually trespassing or intruding into a constitutionally protected area. In *Silverman v. United States*, when the police inserted a microphone inside a house (albeit not far inside), the Court held that the police had intruded into a constitutionally protected area and, therefore, had committed a search within the meaning of the Fourth Amendment.[45] By contrast, in *Goldman v. United States*, when the police used a detectaphone to simply listen in on conversations from a next-door office, without actually entering the office, the Court held that no search had been committed.[46] Likewise, in *Olmstead v. United States*, when the police wiretapped telephone lines located outside of the defendant's house, the Court concluded that there had been no search.[47]

As noted, some Justices dissented from the holdings in these early cases.[48] Justices Brandeis and Murphy sounded the alarm in dissenting

---

39. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 135 (1942), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by Katz*, 389 U.S. 347; *Ex Parte* Jackson, 96 U.S. 727, 733 (1877); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 381 (1974).

40. *See* Weaver*, supra* note 4, at 1134–38.

41. *See Goldman*, 316 U.S. at 134–35.

42. *See Silverman*, 365 U.S. at 506–07.

43. *See Olmstead*, 277 U.S. at 455–57.

44. *See Silverman*, 365 U.S. at 512; *Goldman*, 316 U.S. at 135; *Olmstead*, 277 U.S. at 466.

45. *Silverman*, 365 U.S. at 511–12 ("This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard.").

46. *See Goldman*, 316 U.S. at 135.

47. *Olmstead*, 277 U.S. at 465 ("The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.").

48. *See Goldman*, 316 U.S. at 136–42 (Murphy, J., dissenting); *Olmstead*, 277 U.S. at 471–85 (Brandeis, J., dissenting).

opinions in more than one case.[49] Indeed, in *Silverman*, the Court expressed concern in dicta regarding "the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."[50]

Despite the privacy threats posed by modern technology, the Court took few steps to provide society with protection against advancing technologies until the second half of the twentieth century. In the Court's landmark decision in *Katz v. United States*, issued almost fifty years after the Brandeis and Murphy warnings, the Court attempted to map out a completely new Fourth Amendment approach for handling advancing technologies.[51] In that decision, the Court held that the existence of a Fourth Amendment right did not depend on whether the police had intruded into a "constitutionally protected area," but on whether the government had violated an individual's "expectation of privacy."[52] A concurring Justice Harlan essentially agreed with the Court but argued that the expectation of privacy must be one that society recognizes as "reasonable."[53] The Court ultimately adopted the Harlan formulation.[54]

The *Katz* test *seemed* to provide the courts with a sound basis for dealing with the problem of advancing technology. In *Katz*, the defendant made a phone call from a telephone booth, and the police overheard the conversation using a listening device attached to the outside of the booth.[55] Based on prior precedent, it would have been difficult to argue that the police had conducted a search because most might not regard a phone booth as a protected area (such as a home).[56] Moreover, the government had not "trespassed" into the phone booth because it had simply attached a listening device to the outside to capture sound waves emanating from the booth.[57] In other words, the listening device functioned much like a detectaphone.[58] Despite the absence of a trespass, the Court held that the government's use of the listening device

---

49. *See, e.g.*, *Goldman*, 316 U.S. at 136–42; *Olmstead*, 277 U.S. at 471–85.

50. *Silverman*, 365 U.S. at 509.

51. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

52. *Id.* ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citations omitted)).

53. *Id.* at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

54. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968) (discussing that an individual is free from unreasonable governmental intrusion when he has a reasonable expectation of privacy).

55. *Katz*, 389 U.S. at 349 (majority opinion).

56. *See* United States v. Knotts, 460 U.S. 276, 276–77 (1983) (explaining that placing a beeper in a can located in the person's vehicle and monitoring that person's location is not a Fourth Amendment search if the movements could have been observed by the naked eye).

57. *Katz*, 389 U.S. at 352–53 (explaining that the Government trespassed because it had electronically listened to and recorded the voice of the petitioner inside the booth).

58. *See id.* at 368 (Black, J., dissenting).

qualified as a search because the government had violated Katz's reasonable expectation of privacy (REOP): "One who occupies [a phone 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."[59]

Even though *Katz* seemed to provide a sound basis for evaluating the impact of technology, *Katz*'s promise remains unfulfilled.[60] The Court has struggled to apply the *Katz* formulation in subsequent cases, and the REOP test has not provided much protection against the onslaught of technology.[61] Although the Court has rendered some post-*Katz* technology decisions that are privacy protective, the general thrust of the Court's jurisprudence has been largely unprotective.[62] The problem is the Court has narrowly construed the REOP test.[63] In a series of cases, the Court found that individuals do not have a REOP even though a reasonable person might have concluded otherwise.[64] For example, the Court has held that individuals do not have a REOP in "open fields" even if they are fenced and posted with "no trespassing" signs;[65] against helicopters hovering at very low altitudes over their homes;[66] regarding garbage that they leave on the street for the garbage collector;[67] against canine sniffs of their luggage;[68] and in their automobiles when ground-tracking devices are used to follow their movements in some instances[69] (except when the device is used to uncover information about the inside of a home[70] or when police commit a trespass when installing the device on a vehicle).[71]

---

59. *Id.* at 352 (majority opinion).

60. *See* Weaver, *supra* note 4, at 1164–65.

61. *See id.* at 1153–1227 (explaining that the vague *Katz* test failed to provide subsequent courts with precise direction or guidance).

62. *See* Riley v. California, 134 S. Ct. 2473, 2484–85, 2491 (2014) (holding that the police may not search the electronic contents of an individual's smart phone incident to arrest, despite precedent suggesting that the police can search closed containers as part of such a search); Kyllo v. United States, 533 U.S. 27, 34–37 (2001) (holding that the use of forward-looking infrared technology to determine the amount of heat emanating from a home (to determine whether the owner might be using lights to grow marijuana in his attic) constituted a "search" within the meaning of the Fourth Amendment); Weaver, *supra* note 4, at 1165–66 (explaining that post-*Katz* decisions based on protection of privacy were founded on traditional property principles).

63. *See* Weaver, *supra* note 4, at 1138.

64. *See id.* at 1154–58 (observing that the existence of a REOP depended largely on whether the Justices construed the *Katz* test narrowly or broadly).

65. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 179 (1984) ("[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance.").

66. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451–52 (1989); California v. Ciraolo, 476 U.S. 207, 213–15 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

67. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40–45 (1988).

68. *See, e.g.*, United States v. Place, 462 U.S. 696, 706 (1983).

69. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983).

70. *See, e.g.*, United States v. Karo, 468 U.S. 705, 714–15 (1984).

71. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 945–53 (2012).

As restrictive as these decisions might have been, the Court has issued other, potentially more troubling decisions, holding that there is no REOP for information that is voluntarily conveyed to a third party.[72] For example, in *Smith v. Maryland*, the Court held that the police did not violate an individual's REOP when they installed a pen register at the phone company that allowed them to mechanically record all of the phone numbers dialed by the individual.[73] The Court concluded that an individual has no "legitimate expectation of privacy" in things that he "voluntarily turns over to third parties," including to the phone company's mechanical equipment.[74] The Court noted that the phone company's customers realized that the phone company recorded telephone numbers for various purposes (for example, long distance billing) and concluded that Smith had no REOP in the numbers that he dialed.[75] Likewise, in *United States v. Miller*, the Court held that an individual did not retain a REOP in bank records being held by his bank because he had voluntarily turned the records over to a third party.[76] In *Couch v. United States*, the Court held that a client could not claim a REOP in his own documents that were in the possession of a third party (his accountant).[77]

If broadly applied, the "voluntarily turned over to a third party" doctrine creates a potentially gaping hole in the Fourth Amendment and suggests that the Fourth Amendment provides almost no protection against many modern surveillance methods.[78] For example, consider the NSA's massive surveillance operation, which collects information about emails, texts, and cell phone calls.[79] In a modern technologically driven society, virtually all of these communications are routed through third parties. Emails and text messages are usually sent through internet service providers (ISPs) like Verizon, AT&T, and T-Mobile. Cell phone calls are also routed through third parties. Of course, *Katz* itself involved a phone call placed through the phone company, and the Court concluded that Katz was protected by a REOP.[80] In light of decisions like *Smith*, *Miller*, and *Couch*, it is not clear

72. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744–45 (1979); United States v. Miller, 425 U.S. 435, 442 (1976); Couch v. United States, 409 U.S. 322, 335 (1973).

73. *Smith*, 442 U.S. at 745–46.

74. *Id.* at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

75. *See id.* at 744–45.

76. *Miller*, 425 U.S. at 440–44 (noting that Miller could not assert either ownership or possession over the records since the bank was required to keep them pursuant to its statutory obligations).

77. *Couch*, 409 U.S. at 335 ("[T]here can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return.").

78. *See, e.g.*, *id.*

79. *See* Shane, *supra* note 18.

80. Katz v. United States, 389 U.S. 347, 359 (1967).

that emails, phone calls, and text messages are accompanied by a REOP today.[81]

IV. HOPEFUL SIGNS FOR THE FUTURE?

There is some hope that the Court will alter its jurisprudence in a way that comes to grips with new technologies. Indeed, in a couple of recent decisions, the Court has chosen to provide greater protection against police attempts to use technology to invade individual privacy.[82] For example, in *Kyllo v. United States*, the Court held that the police violated a homeowner's REOP when they used forward-looking infrared technology (FLIR) to determine the amount of heat emanating from his home (the police used FLIR to confirm their suspicion that the occupants were using special lights to grow marijuana in their attic).[83] The Court was concerned that the police used technology to gain "information regarding the interior of the home that could not otherwise have been obtained without" intruding into the house.[84] The Court, however, qualified its holding by emphasizing that the police had used technology that was "not in general public use."[85] Likewise, in *Florida v. Jardines*, the Court held that the police committed a search when they entered the curtilage of Jardines's home to have a narcotics-detection dog sniff at his front door.[86] In that case, however, the Court did not apply the REOP test but instead focused on the fact that the officers and the dog committed a physical intrusion into the constitutionally protected area of the curtilage of the defendant's home.[87] The difficulty is that, despite the Court's protectiveness towards the home, it has provided little protection against governmental surveillance of communications sent outside a person's home.

Another difficulty is that neither *Kyllo* nor *Jardines* articulated a satisfactory replacement for the *Katz* test.[88] Individual Justices have expressed concern regarding the impact of technology on privacy and have suggested that the Court needs to come up with a new approach.[89] Illustrative is *City of Ontario v. Quon*.[90] Although Quon did not present a compelling privacy case (a member of a police SWAT team argued that he had a REOP in text messages that he sent and received on a wireless pager issued by the City for his use and for work-related purposes), the Court assumed that Quon

---

81. *See supra* notes 72–77 and accompanying text.

82. *See* Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013); Kyllo v. United States, 533 U.S. 27, 40 (2001).

83. *Kyllo*, 533 U.S. at 40.

84. *Id.* at 34.

85. *Id.*

86. *Jardines*, 133 S. Ct. at 1417–18.

87. *Id.* at 1416–17.

88. *See id.* at 1417; *Kyllo*, 533 U.S. at 34–35.

89. *See supra* notes 12–16 and accompanying text.

90. City of Ontario v. Quon, 560 U.S. 746, 764–65 (2010).

had a reasonable expectation of privacy in his messages, it expressed hesitance to establish fixed rules regarding the application of Fourth Amendment rules to emerging technologies: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[91] In some respects, this hesitance was staggering. After all, the Court had been struggling with the implications of technology for nearly a century, and one would have hoped that it would have been able to come up with clearer guidelines by that time. Of course, there was some sense in the *Quon* Court's observations. As the Court noted, the "dynamics of communication and information transmission" are changing rapidly, as are societal expectations regarding what should be regarded as proper and improper behavior, and the Court worried about its ability to predict "how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable."[92]

Perhaps the most hopeful decision was rendered in *Riley v. California*, a case in which the Court held that the police could not routinely search digital information on a cell phone as part of a search incident to legal arrest.[93] In one of the fact scenarios presented in that case, an officer stopped Riley for driving with expired license plates, arrested him when the officer became suspicious that he was associated with gang activity, and searched his smart phone pursuant to the search incident to legal arrest doctrine.[94] Although the Court reaffirmed the validity of the exception, the Court invalidated this particular search.[95] In doing so, the Court emphasized that individuals are entitled to privacy against governmental intrusion into their private affairs and described smart phones as "minicomputers" that have multiple functions, including the ability to perform like telephones as well as like "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and can store "millions of pages of text, thousands of pictures, or hundreds of videos."[96] By using a smart phone, the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions" that can reveal a user's Internet searches, browsing history, and personal movements.[97] As a result, the Court regarded a search of a smart phone as quite different than the pen register used in *Smith v. Maryland*.[98]

---

91. *See id.* at 759.
92. *Id.* at 759–60.
93. Riley v. California, 134 S. Ct. 2473, 2485 (2014).
94. *Id.* at 2480.
95. *Id.* at 2495.
96. *Id.* at 2489.
97. *Id.*
98. *Compare id.* at 2492–93 (finding that the "officers engaged in a search of [the defendant's] cell phone" because more than just phone numbers could be found), *with id.* at 2492 (discussing the holding in *Smith v. Maryland* that "no warrant was required to use a pen register . . . to identify numbers dialed by

In *Riley*, in evaluating the validity of the government's action, the Court balanced "the degree to which [a search] intrudes upon an individual's privacy" against "the degree to which it is needed for the promotion of legitimate governmental interests."[99] Since the "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape," the Court concluded that the police could not search it except to determine whether it contained a concealed weapon (like a razor blade).[100] Even though the Court was aware of the fact that a smart phone might be vulnerable to two different types of evidence destruction—remote wiping and data encryption—the Court viewed these concerns as remote given that the government had offered nothing more than "a couple of anecdotal examples of remote wiping triggered by an arrest."[101] Regarding encryption, the Court noted that the police would have limited opportunities to search a password-protected phone because smart phones "lock at the touch of a button or, as a default, after some very short period of inactivity."[102] In any event, the police can prevent remote wiping "by disconnecting a phone from the network," which can happen by removing the battery or placing the phone in a bag "that isolates [it] from [receiving] radio waves."[103] If there is evidence suggesting that a remote wipe is imminent, the police may be able to establish "exigent circumstances" that would justify an immediate warrantless search.[104]

Riley's pro-privacy holdings and statements offer U.S. citizens some hope that the Court will eventually provide individuals with protection against NSA surveillance of email, text, and phone communications. However, the decision does not inevitably lead to that result. Even if the Court precludes the police from reviewing the contents of an individual's smart phone, it might not go so far as to prohibit the NSA from accessing communications sent by an individual through an ISP or cell phone provider that is remotely situated from the individual's smart phone. As a result, *Riley*

---

a particular caller" and finding that the use of the pen register was not a search under the Fourth Amendment).

99. *Id.* at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

100. *Id.* at 2485.

101. *Id.* at 2486–87.

102. *Id.* at 2487. Moreover, in situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked phone, it is not clear that the ability to conduct a warrantless search would make much of a difference. *See id.* The need to effect the arrest, secure the scene, and tend to other pressing matters means that law enforcement officers may well not be able to turn their attention to a cell phone right away. *See* Transcript of Oral Argument at 50, *Riley*, 134 S. Ct. 2473 (No. 13-132); Brief for United States as Amicus Curiae Supporting Respondent at 19, *Riley*, 134 S. Ct. 2473 (No. 13-132), 2014 WL 1389032. Cell phone data would be vulnerable to remote wiping from the time an individual anticipates arrest to the time any eventual search of the phone is completed, which might be at the station house hours later. *See Riley*, 134 S. Ct. at 2487. Likewise, an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted. *See id.* at 2486.

103. *Riley*, 134 S. Ct. at 2487.

104. *Id.*

does not definitively resolve the Fourth Amendment issues raised by the NSA surveillance program and does not come to grips with the Court's prior precedent which suggests that there is no REOP in information that an individual voluntarily turns over to a third party. It is unclear whether and how the Court will apply its precedent to smart phones and computers or to communications made through such devices.

Even if the Court's Fourth Amendment jurisprudence were construed broadly enough to allow an individual to challenge the government's seizure of phone call information, texts, or emails, a potentially aggrieved individual might not be able to bring suit. For one thing, the individual may not be able to prove that he is under surveillance. As noted, when the NSA sends a National Security Letter to a telecommunications company, it usually includes an order precluding the company from publicly acknowledging the letters or the disclosures, or even from alerting their customers.[105] Moreover, to bring suit, individuals must be able to establish standing in the sense of establishing sufficient injury to satisfy the Article III case or controversy requirement.[106] In *Clapper v. Amnesty International USA*, individuals who were the likely targets of NSA surveillance (they were providing legal representation to alleged terrorists who had been detained at Guantanamo Bay) sought to challenge the NSA's cyber-surveillance program.[107] Because of the secrecy that pervaded the NSA program, however, the plaintiffs were unable to prove they were actual targets of the NSA program, and the Court concluded that they could not establish injury or standing to sue.[108]

Of course, the *Clapper* decision placed potential plaintiffs in an almost impossible situation. To have standing to sue, plaintiffs must be able to prove that the NSA is subjecting them to surveillance.[109] The NSA, however, goes to great lengths to maintain secrecy regarding the scope of its surveillance program.[110] As a result, it is extremely difficult for individuals to prove that they are the targets of governmental surveillance. In *Clapper*, the plaintiffs asked that the Government be forced to reveal, through in camera proceedings, whether it was intercepting the plaintiffs' communi-cations, as well as the targeting procedures the Government was using.[111] The Court refused to require the Government to make this revelation, noting that plaintiffs were required to establish standing by "pointing to specific facts," and that the Government was not required to "disprove standing by revealing details of its surveillance priorities."[112] The plaintiffs could not prove that they were under surveillance because of the super-secret nature of the

105. *See* Shane, *supra* note 18; Stanglin, *supra* note 18.
106. *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).
107. *Id.* at 1138.
108. *Id.* at 1148–55 (citing Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2752 (2010)).
109. *See id*. at 1147–50.
110. *See id.*
111. *Id.* at 1149 n.4.
112. *Id.*

government's surveillance program, and therefore could not meet the case or controversy requirement necessary to proceed with the litigation.[113]

V. CONCLUSION

Although advances in technology have completely transformed society in recent decades, including and especially police surveillance techniques, society and the courts have not kept pace with advances in surveillance techniques.[114] In the Fourth Amendment area, for many years, the Court's analysis was mired in a historical approach that focused on whether the police had intruded into a constitutionally protected area.[115] Even though this approach may have worked well for the founding generation, it provided little protection against the onslaught of modern technologies. As technology allowed the police to snoop on people without actually entering constitutionally protected areas, the Court's Fourth Amendment approach began to break down.

In its landmark decision in the *Katz* case, the Court attempted to come to grips with the difficulties presented by advancing technologies.[116] In that case, the Court suggested that the definition of a search was not limited to situations when the government intruded into a constitutionally protected area but included situations when the police intruded on an individual's reasonable expectation of privacy.[117] The difficulty is that the *Katz* test has been rather narrowly construed. Although it has provided protection against new technologies in a limited number of cases (for example, protection against police use of FLIR technology to determine the level of heat emanating from a home), in general, courts have restrictively construed the decision and have provided little protection.[118] Moreover, under the *Katz* test, the Court has suggested that the Fourth Amendment provides no protection for information voluntarily turned over to a third party. Since most modern communications are routed through third parties, the third-party exception seems to rip a gaping hole in the Fourth Amendment. Virtually all NSA surveillance involves information that has been communicated to, and through, third parties.

All is not lost. In *Riley*, the Court held that the police may not search smart phones incident to the arrest of a motorist.[119] *Riley* suggests that the Court is becoming more acutely aware of the problems presented by modern technologies, which gives the citizenry hope that the Court's future decisions

113. *Id.* at 1154.
114. *See supra* Part III.
115. *See supra* Part III.
116. *See supra* notes 51–52 and accompanying text.
117. *See* Katz v. United States, 389 U.S. 347, 351 (1967).
118. *See supra* Part III.
119. Riley v. California, 134 S. Ct. 2473, 2485 (2014).

will expand Fourth Amendment jurisprudence to deal with such technologies.[120] On the other hand, the Court has been struggling with the problem of advancing technologies in the Fourth Amendment area for more than a century and has made little headway. One can only hope that the Court will be more successful in the coming years. If not, the Fourth Amendment will provide the citizenry with little protection against the NSA cyber-surveillance program.

120. *See supra* Part IV.