Harvard Journal of Law & Technology
Volume 28, Number 2 Spring 2015

HOMING IN: TECHNOLOGY'S PLACE IN FOURTH AMENDMENT JURISPRUDENCE

*Emma Raviv**

TABLE OF CONTENTS

I. INTRODUCTION

Fourth Amendment law is often called "unruly" because "[w]ith so many decided cases and so few agreed-upon principles at work, trying to understand the Fourth Amendment is a bit like trying to put together a jigsaw puzzle with several incorrect pieces: No matter which way you try to assemble it, a few pieces won't fit."[1] One potential reason for this unruliness is that technological innovation has thrown a wrench into the Fourth Amendment's legal development. As

* Harvard Law School, J.D. 2014; University of Maryland, B.A. 2010. Thanks to Professor Phillip Heymann for his encouragement and support in developing this Note. Thanks also to Travis West, for his patient efforts at improving it. Finally, thanks to the staff of the *Harvard Journal of Law and Technology* for all their hard work in bringing this Note to print.

1. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004); *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994) (calling Fourth Amendment jurisprudence "a vast jumble of judicial pronouncements that is not merely complex and contradictory, but often perverse.").

soon as one method of crime-solving is implemented and accepted, a newer, more advanced, and potentially more intrusive version debuts that sets us all back on edge, and back into a position of constitutional uncertainty.

For its part, the Supreme Court has faced and answered difficult questions about technology's role in privacy and criminal procedure in a generally satisfying manner. Through its holdings, the Court has generated two clear rules pertaining to technology in this space.[2] First, it has made clear that government agencies using technology to gain access to and gather data from a traditionally protected (private) space without a warrant will not be tolerated.[3] Second, no government will be allowed to engage in warrantless physical trespass upon the property of the defendant in order to gather information.[4] The coupling of these two rules, combined with the more flexible "reasonable expectation of privacy" test, yields decisions regarding technology that are generally sensible because Justices need not understand the mechanics of technology to apply them.[5] They also foster other benefits: flexibility in the face of new innovation and administrability for law enforcement.[6]

A danger lies, of course, in the areas that escape these clear delineations. Further innovation will continue to challenge the Court if its gaps are left unfilled, which may be a slow process absent a one-size-fits-all scheme.[7] Part II outlines what constitutes a search under the Fourth Amendment. Part III discusses the two bright-line rules that the Court has handed down. Part IV addresses the strengths of those bright-line rules, and why we may not need, or want, more guidance at this stage. Part V analyzes the challenges posed by the application of the reasonable expectation of privacy test in general, and also specific technologies and situations left uncovered by the Court's articulated rules: DNA, encryption, and extreme sense-enhancing technology in public spaces. Part VI concludes.

II. FOURTH AMENDMENT: WHAT IS A SEARCH?

The text of the Fourth Amendment offers the following protections:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no

2. *See* discussion *infra* Part III.
3. *See* discussion *infra* Part III.A.
4. *See* discussion *infra* Part III.B.
5. *See* discussion *infra* Part IV.A.
6. *See* discussion *infra* Part IV.B–C.
7. *See* discussion *infra* Part V.

> 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.[8]

In other words, the government must acquire a warrant supported by probable cause in order to conduct searches and seizures, and illegally obtained evidence will be excluded from court proceedings.[9] Held to apply to the states in 1961,[10] the Fourth Amendment has courts ask a series of questions to determine whether government activity is constitutional. Since the Amendment protects against searches and seizures, courts first ask a threshold question: Has a search occurred at all?[11]

Originally, this question would be answered in the affirmative only when cases involved physical intrusions onto private property. In *Olmstead v. United States*,[12] the Court held warrantless wiretaps constitutional because no physical intrusion on private property took place — rather, the equipment was placed in the streets and in the basement of an office building that the defendants did not own.[13] Therefore, "[t]here was no entry of the houses or offices of the defendants."[14]

In 1967, the Court extended Fourth Amendment protection considerably. In *Katz v. United States*,[15] Justice Harlan, in a concurrence later adopted as the controlling opinion, expanded the focus to individual privacy by stating that a search had occurred when the government wiretapped a telephone booth by placing a listening device on the outside of the booth's glass. "[T]he Fourth Amendment protects people — and not simply 'areas' — against unreasonable searches and seizures."[16] Katz was entitled to protection in this instance because he expected privacy when having his conversation in the phone booth, and society believed that expectation to be reasonable. And thus the test was developed: A search has occurred when (1) a person has "exhibited an actual (subjective) expectation of privacy," and (2) society is prepared to recognize that this expectation is (objectively) reasonable.[17] Since it is difficult to contest subjective

---

8. U.S. CONST. amend. IV.

9. Weeks v. United States, 232 U.S. 383, 398 (1914).

10. Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that the Fourth Amendment applies to the states by way of the Due Process Clause of the Fourteenth Amendment).

11. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (discussing whether surveillance without trespass constituted a search).

12. 277 U.S. 438 (1928).

13. *Id.* at 457.

14. *Id.* at 464.

15. 389 U.S. at 361.

16. *Id.* at 353 (Harlan, J., concurring).

17. *Id.* at 361.

expectations of privacy, the primary question in these analyses is what makes an expectation of privacy objectively reasonable.[18] In modern Fourth Amendment jurisprudence, a majority of the Court has adopted a rights-based approach to this question: "[W]hether a 'reasonable' or 'legitimate' expectation of privacy exists depends not on the likelihood that secrets will remain secrets, but upon whether a given individual has an enforceable right to enjoin others from invading her privacy."[19] Until very recently,[20] most cases turned on this so-called right to privacy based on a legitimate, or reasonable, expectation of privacy.

III. ARTICULATED RULES

The Court has articulated two clear rules in the Fourth Amendment realm when it comes to technology. The two rules are undeniably interrelated, but still bear on different cases. The first is that when the government combines technology with data gathering in a place historically considered to be private (i.e., the home), it must obtain a warrant — such activity constitutes a search under the Fourth Amendment.[21] Second, use of technology combined with a physical intrusion upon private property (subject to some exceptions) also constitutes a search and therefore requires a warrant.[22]

A. Technology and Historically Private Places

One certainty in Fourth Amendment doctrine is that the home, and anything within its "curtilage,"[23] is the ultimate private place, and law enforcement cannot use technology to gather data about activities inside of it without obtaining a warrant. Indeed, "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[24]

---

18. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 507 (2001).

19. *Id.* at 508. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109 (1984) (holding that no warrant was needed to field test defendant's white powder substance to ascertain that it was cocaine, because cocaine is contraband and so no extraconstitutional right to stop the government's test existed); Florida v. Riley, 488 U.S. 445 (1989) (holding that a fence erected around marijuana plants did not create a reasonable expectation of privacy when the plants were still visible from public airspace).

20. *See infra* Part III.B.

21. *See* discussion *infra* Part III.A.

22. *See* discussion *infra* Part III.B.

23. The plain English definition is, "the area of land occupied by a dwelling and its yard and outbuildings, actually enclosed or considered as enclosed." *Definition of Curtilage*, DICTIONARY.COM, http://dictionary.reference.com/browse/curtilage?s=t (last visited May 9, 2015).

24. Silverman v. United States, 365 U.S. 505, 511 (1961).

The first cases that addressed technology and the home concerned airplane flyovers. In *Dow Chem. Co. v. United States*,[25] the Court held that taking photographs in an airplane flyover of an industrial complex is not an impermissible search. Naked-eye surveillance of even a home's backyard does not amount to a search;[26] technology — flight and high-resolution cameras — does not change that calculus, particularly when the area observed is *not* a home.[27] *Florida v. Riley*[28] took the same concept a little closer to home: In that case, the government flew a helicopter at a low altitude and, in doing so, saw marijuana plants in a partially covered greenhouse. Again, the Court determined that this was not a search. First, Federal Aviation Authority regulations allow aircraft to fly above homes, so the plants were in plain view; anything the public can see from a public place is not entitled to a reasonable expectation of privacy.[29] Moreover, no intimate details were observed from the helicopter.[30]

How far a home's boundaries extend rests on the curtilage doctrine. An area will be within the curtilage of a home if it harbors the "intimate activity associated with the 'sanctity of a man's home and the privacies of life.'"[31] In assessing whether an area is included in the curtilage of the home, courts look to distance, enclosure by fences, the nature of the use, and the level of protection from observation.[32] While a barn sixty yards away from a home was not considered to be within the home's curtilage,[33] a porch in front of a house was, despite the fact that Girl Scouts and salespeople are allowed to enter it to knock on the door.[34]

Kyllo v. United States[35] is the most recent capstone case in this area, and the clearest articulation of the bright privacy line that exists at the entrance to the home. In 1992, authorities used a thermal imaging device to analyze the home of Danny Kyllo under suspicion that his neighbor was involved in the manufacture of marijuana. The of-

---

25. 476 U.S. 227 (1986).

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

27. *See* Dow Chem. Co., 476 U.S. at 238–39 (treating the use of high-resolution cameras in aerial surveillance as irrelevant in the Fourth Amendment inquiry, particularly when an industrial complex is not considered to be within a home's curtilage). The Court left open the possibility "that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the general public" might raise Fourth Amendment issues. *Id.* at 238. However, the Court did not find the photographic technology here to be troubling, since "[t]he mere fact that human vision is enhanced somewhat . . . does not give rise to constitutional problems." *Id.*

28. 488 U.S. 445 (1989).

29. *Id.* at 449.

30. *Id.* at 452.

31. Oliver v. United States, 466 U.S.170, 180 (1984) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

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

33. *Id.* at 302.

34. Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013).

35. 533 U.S. 27 (2001).

ficer grew suspicious of Kyllo and compared Kyllo's utility records to averages, and his electricity usage was higher — consistent with use of marijuana heat lamps.[36]

In 1992, nobody had authoritatively decided whether use of thermal imaging devices constituted a search — in other words, whether aiming the camera at someone's home would require a warrant. The sergeant investigating the heat signatures in Kyllo's house assumed it would not.[37]

What he found was that Kyllo's garage roof and a sidewall were relatively hot compared to the rest of his home and substantially warmer than the neighboring units.[38] Based in part on the thermal imaging, a federal magistrate judge issued a warrant to search Kyllo's home, where the investigating agents found marijuana plants.[39] After being indicted on a federal drug charge, Kyllo unsuccessfully moved to suppress the evidence seized from his home. The Ninth Circuit, refusing to assess future capabilities of similar technology, affirmed: "Whatever the 'Star Wars' capabilities this technology may possess in the abstract, the thermal imaging device employed here intruded into nothing."[40] Rather, the camera measured heat emissions radiating from — and therefore outside — the home, and Kyllo did not attempt to conceal them.[41] Therefore Kyllo had no subjective expectation of privacy, and, even if he had attempted to conceal the heat, there was no objectively reasonable expectation of privacy because the thermal imager did not expose any intimate details of his life — just "amorphous 'hot spots.'"[42]

The Supreme Court reversed, rejecting the Ninth Circuit's "mechanical" approach to what thermal imaging technology does.[43] Writing for the majority, Justice Scalia refused to endorse the idea that these devices detect only heat radiating from the home's external surface the same way that eavesdropping devices pick up only sound waves that reach the exterior of a phone booth, an argument summarily rejected in *Katz*.[44] But most importantly, the Court held that the home is sacred, and technology should not be allowed to encroach upon it without a warrant.[45]

In this case, then, it is simple: Using technology that is not in general public use, to gain information that would otherwise remain

36. United States v. Kyllo, 190 F.3d 1041, 1043–44 (9th Cir. 1999).
37. *Kyllo*, 533 U.S. at 29–30.
38. *Id*. at 30.
39. *Id.*
40. Kyllo, 190 F.3d at 1046.
41. *Id.*
42. *Id.* at 1047.
43. *Kyllo*, 533 U.S. at 40.
44. *Id*. at 35.
45. *Id.* at 40.

inaccessible without a physical intrusion into a home, is a search.[46] "[T]he Fourth Amendment draws a firm line at the entrance to the house. That line, we think, must be not only firm but bright."[47]

While drawing that bright line at the entrance to a home, Justice Scalia also addressed, for the first time, the challenges of technological innovation head on: "While the 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."[48] Innovation, then, served as a reason for caution. The Court did note, however, that even in its crude form, thermal imaging could reveal intimate details: The device might disclose "at what hour each night the lady of the house takes her daily sauna and bath."[49] Of course, such intimate details would be accessible only because the thermal imaging device was being directed at a home, rather than any other building or vehicle, again highlighting the narrowness of the holding.

This bright line rule is not without critique — even within the *Kyllo* opinions. Dissenting, Justice Stevens questioned why the home should be so different, because if the technology can identify criminal conduct and nothing more, then it should not receive protection.[50] As such, he argued the holding was too broad. Additionally, per *Katz*, the limitation to protection of the home was also too narrow, since the expectation of privacy clearly extends to a phone booth and other non-home places. What Justice Stevens's point misses is the jigsaw puzzle nature of the Court's rules pertaining to the Fourth Amendment. *Kyllo* and the other cases in this section show that, aside from all else, the home is different, and a line exists at its entrance that the government simply cannot cross.[51]

---

46. *Id.* at 34–35.

47. *Id.* at 40 (internal quotations and citations omitted).

48. *Id.* at 36.

49. *Id.* at 38.

50. *Id*. at 47–48 (Stevens, J., dissenting); *see also* United States v. Place, 462 U.S. 696, 707 (1983) (holding that a dog sniff does not constitute a search under the Fourth Amendment because it is intended to reveal only the presence or absence of narcotics). Thermal imaging does not appear to fall into this exception at any rate, since the ownership of something that emanates heat, on its own, is not criminal conduct. The bathing example bears this out. *See Kyllo*, 533 U.S. at 38.

51. A counterexample here is the third-party doctrine, which legally eliminates the expectation of privacy in information communicated to any third party. Smith v. Maryland, 442 U.S. 735, 743–44 (1979). Kyllo likely would have believed that he had an expectation of privacy in thermal imaging of his home and also his phone metadata; after all, both of these originated in the home. Still, authorities would be able to subpoena records from the phone company for phone metadata without violating Kyllo's Fourth Amendment rights. The difference might be that, in the case of phone metadata, there are specific receivers Kyllo would have known about. Further analysis, however, is beyond the scope of this Note.

B. Technology and Physical Trespass

The second clear rule the Court has articulated in this sphere is that physical trespass onto someone's protected property constitutes a search and therefore requires a warrant. Long dormant, this rule was revived by *United States v. Jones*.[52]

Antoine Jones was arrested in late 2005 for drug possession after police attached a global positioning system ("GPS") tracking device to his vehicle, and subsequently used it to monitor his movements on public streets for twenty-eight days, amassing more than 2000 pages of data.[53] Before trial, Jones filed a motion to suppress the evidence obtained from the GPS device, but the district court held that the data obtained while on public thoroughfares was admissible because a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[54]

At trial, the government introduced the data obtained from the GPS, which connected Jones to the alleged conspirators' house where they stored their drugs.[55] The jury found Jones guilty of conspiracy to distribute and possess with intent to distribute cocaine, and the court sentenced him to life imprisonment.[56] The D.C. Circuit reversed the conviction; it found that the warrantless installation of a GPS device violated the Fourth Amendment, and therefore the data derived from it must be excluded.[57]

The Supreme Court affirmed. Writing for the majority, Justice Scalia held that the placement of the GPS tracker constituted a search because the government occupied private property in placing it: It was a physical intrusion.[58] Justice Scalia, perhaps unsurprisingly, made reference to the text of the Fourth Amendment to support his holding — that the Fourth Amendment is closely connected to property, "since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, paper, and effects' would have been superfluous."[59]

Justice Scalia also referenced the Fourth Amendment's roots in common-law trespass. Despite the clear shift, begun by *Katz*, away from this approach, the Fourth Amendment's protection against tres-

52. 132 S. Ct. 945 (2012).
53. *Id.* at 948.
54. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006).
55. *Jones*, 132 S. Ct. at 948–49.
56. *Id*. at 949.
57. *Id.* at 948–49.
58. *Id.* at 949.
59. *Id.*

pass remained unchanged. In *Soldal v. Cook County*,[60] the Court explained that *Katz* established that "property rights are not the sole measure of Fourth Amendment violations," but did not "snuff[] out the previously recognized protection for property."[61] Many cases post-*Katz* stated that *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."[62]

A number of cases, seemingly similar to *Jones*, had been decided the other way. The one distinguishing factor was the presence of physical trespass. In *United States v. Knotts*, a "beeper" had been placed in a container of chloroform to track the movements of the vehicle in which it was placed.[63] The case was decided on reasonable expectation of privacy grounds because there was no physical trespass: The beeper was placed in the container before it came into Knotts's possession, with the consent of the then-owner.[64] In *United States v. Karo*,[65] the Court directly addressed the question left open by *Knotts*: whether installation of a beeper into such a container constituted a search. The Court found that it did not.[66] Both Knotts and Karo accepted the containers as they came to them, whereas Jones owned his Jeep at the time the government trespassed upon it and installed the GPS device.

Justice Scalia made clear that visual surveillance of Jones's car would not present a Fourth Amendment problem. The outside of a vehicle is, indeed, presented to the public, but the police officers were doing much more than visual surveillance when installing the GPS device: They physically encroached on a protected area.[67] The majority thought that traditional visual surveillance of Jones for a four-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance, . . . [but the] cases suggest that such visual observation is constitutionally permissible."[68]

---

60. 506 U.S. 56 (1992).

61. *Id.* at 64.

62. *Jones*, 132 S. Ct. at 951 (citing United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) (internal quotation marks omitted)).

63. *Knotts*, 460 U.S. at 278.

64. *Id.* at 278, 285.

65. 468 U.S. 705 (1984).

66. *Id.* at 712.

67. *Jones*, 132 S. Ct. at 952.

68. *Id.* at 953–54. Notably, the Court leaves unanswered the question of whether using technological means to conduct surveillance of this nature, in the absence of a trespass, is an unconstitutional invasion of privacy. *Id.* at 956. Despite past cases' suggestion that visual observation, no matter how intense, would be constitutional, the concurrences suggest that long-term surveillance would violate the *Katz* "reasonable expectation of privacy" standard. *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

Justice Scalia additionally clarified that the physical trespass test is not the exclusive test.[69] Other situations that do not implicate physical trespass on protected areas are still subject to *Katz*'s reasonable expectation of privacy analysis.[70] As such, the Court added (or, perhaps more accurately, explicitly revived) a rule with which to assess *some* Fourth Amendment cases.

This articulated rule could be tricky when it is unclear whether the property being intruded upon is protected. The rule clearly applies to one's home, but it does not so clearly apply to one's private park. However, the cases offer some guidance on this issue. This question generally turns on whether the property is within the curtilage of home, as discussed *supra*, and whether the property at issue can be considered to be an open field. Such open fields, even if on private property, are not protected. In *Oliver v. United States*,[71] the Court found that the government's entrance onto a field was a trespass at common law, but "open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields."[72] Therefore, no search had occurred. Regarding other structures on someone's property, the Court ruled in *Dunn* that a barn, sixty yards away from the defendant's house, not fenced in, and with windows through which people could see, was not within the curtilage of home, so the physical trespass did not amount to a search.[73]

IV. THE RULES' STRENGTHS

Though patchwork in nature, the two rules the Court has articulated work when applied to many technology-based Fourth Amendment cases. These rules are successfully applied and implemented because the rules do not require Justices to understand exactly how the technology at issue works, they allow flexibility in the face of speedy innovation, and they are clear enough to be administrable by law enforcement.

A. Capabilities, Not Mechanics

As a general proposition, courts struggle with new technology, and the Supreme Court is no exception. When confronted with com-

69. *Id*. at 953.
70. *Id*.
71. 466 U.S. 170 (1984); *see also* Hester v. United States, 265 U.S. 57 (1924).
72. *Oliver*, 466 U.S. at 179.
73. United States v. Dunn, 480 U.S. 294, 305 (1987).

plex science and technology, judges sometimes ask questions at oral argument that betray a lack of understanding, even though "as members of the nation's highest court, [the Justices] are increasingly asked to set legal precedents about these very technologies."[74] The technology-related precedents are not confined to the Fourth Amendment: The 2010–2011 term, for example, had the Court facing cases concerning the Freedom of Information Act, copyright, the state secrets privilege, and freedom of expression.[75] Some believe the Court is younger and more technology-familiar than ever before: "You're getting a new generation of justices. You've got justices who text on their phones, who do e-mail, who actually use a computer," said Thomas Goldstein, the founder of SCOTUSblog.[76]

But how true is this statement? In a 2010 opinion, Justice Kennedy expressed doubts about the Court's knowledge and experience regarding text messaging.[77] Justice Thomas has said that the Court is in "catch up mode in the area of technology."[78] Justice Scalia has called himself "Mr. Clueless" when it comes to new media technology.[79] Chief Justice Roberts has called search engines "search stations" in an oral argument.[80] More recently, Justice Sotomayor referred to "iDrop," and admitted that "this [technological nuance] is really hard for me."[81] The blunders have been numerous, and often concern technology Americans rely on every day.[82]

The dangers of this ignorance can be very real. Supreme Court Justices "have to rule on every subject under the sun,"[83] and particularly in areas like patent and copyright, the technology *is* the subject being litigated, and how the technologies work is "a key part of the cases' facts."[84] However, in the Fourth Amendment arena, exactly

---

74. Mark Grabowski, *Are Technical Difficulties at the Supreme Court Causing a "Disregard of Duty"?*, 3 CASE W. RES. J.L. TECH. & INTERNET (2012).

75. David Kravets, *All Rise: Supreme Court's Geekiest Generation Begins*, WIRED (Oct. 1, 2010), http://www.wired.com/threatlevel/2010/10/supreme-court-2010-2011-term.

76. *Id.*

77. City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground." (citations omitted)).

78. Roy M. Mersky & Kumar Percy, *The Supreme Court Enters the Internet Age: The Court and Technology*, LLRX (June 1, 2000), http://www.llrx.com/features/supremect.htm.

79. Jordan Fabian, *Chairman to Justices: "Have Either of Y'all Ever Considered Tweeting or Twitting?,"* HILL (May 21, 2010, 3:30 PM), http://thehill.com/policy/technology/99209-chairman-to-justices-have-either-of-yall-ever-considering-tweeting-or-twitting-.

80. Transcript of Oral Argument at 36, Bilski v. Kappos, 561 U.S. 593 (2010) (No. 08-964).

81. Transcript of Oral Argument at 8, 12, Am. Broad. Cos., v. Aereo, Inc., 134 S. Ct. 2498 (2014) (No. 13-461).

82. Grabowski, *supra* note 74, at 95. However, to be fair to the Justices, several of these errors occurred in oral arguments where Justices may be less precise.

83. *Id.* at 100.

84. *Id.*

how the technology works is less relevant to the legal analysis. Rather than understanding the technical details of the devices implicated, the Justices need only understand the potential capabilities and ramifications of the technology.

Potential capabilities and impact are easier than mechanics for non-scientists to understand. One does not need a master's degree in electrical engineering to know how light bulbs have impacted society, nor does one need to know how to code in order to assess the extent to which the Internet and social media have changed Americans' sharing practices. As Rebecca Tushnet points out, "the issue is more of understanding how different social groups experience the world than of the details of the technologies in themselves."[85] Justices' perception of how the world works with technology impacts their analysis on some Fourth Amendment issues, namely when assessing whether an expectation of privacy is reasonable. And, without a doubt, most of the Supreme Court Justices use technology less, or differently, than many Americans. However, that the Justices do not themselves use Twitter does not prevent them from understanding that others do and from receiving evidence on the topic. That level of unfamiliarity cannot possibly exceed their unfamiliarity with many other topics the Court faces in which the Justices never had formal schooling, like statistics, police deterrence and psychology, or patents.

Mark Grabowski attributes great significance to the Justices' technological ignorance, stating that because of a lack of technological understanding, "cases involving technological issues may face the worst odds of being addressed by the current Court, despite the fact that the legal questions they raise may be the most pressing given their novelty and the lack of precedents."[86] But such alarm assumes that Justices do not consult with anyone else when selecting cases — an assumption that simply is not true. The Supreme Court clerks' biggest job is to sort through the petitions for certiorari, drafting memoranda recommending whether or not to grant a petition.[87] Unlike the Justices, the clerks are young and conversant in technology and can

85. *Id.* at 102.

86. *Id.* at 105. *But see* Dennis Crouch, *Supreme Court Patent Cases per Decade*, PATENTLY-O (July 30, 2014), http://patentlyo.com/patent/2014/07/supreme-patent-decade.html (finding that the Supreme Court has heard more patent cases since 2010 than in each of the preceding four decades).

87. Richard Wolf, *About 2,000 Petitions Await Supreme Court's Return*, USA TODAY (Sept. 23, 2013), http://www.usatoday.com/story/news/nation/2013/09/23/supreme-court-petitions-prisoners-clerks/2843401/ ("Thankfully, the justices have had help whittling down the pile of petitions. Their law clerks — 36 young men and women, most in their 20s and hailing from the nation's top-ranked law schools — have been writing memos on each case and recommending only the most consequential for consideration.").

identify when consequential technology-based cases arise, even if the Justices themselves cannot.[88]

The documented misunderstanding of communications technology, then, likely does not impact how Justices select cases and deal with surveillance technology like GPS, heat-detection devices, and high definition cameras. Instead of having to ask, for example, how infrared works, the Justices need to ask questions like: How many people have access to this technology? What role does this technology play in law enforcement writ small, and American society writ large? How does this technology impact what kinds of information the government can gather about individuals, on both qualitative and quantitative levels? What analogies can be drawn between new and existing capabilities?[89]

B. Piecemeal Rules May Be the Best Way To Deal with Evolving Technology

Sometimes the previous questions are not easy to answer, because how technology evolves is not always predictable. New technology systems are likely to have unintended side effects, can unpredictably fail, and often require complex decisions as to use. Additionally, technical facts are often unknown or unavailable,[90] which makes societal impact particularly difficult to predict.[91] However, the Justices are not generally left to speculate on these topics. First, by the time the relevant cases come before them, it is clear how the technology is being used by law enforcement at the time — that is, the technology is no longer brand new and society is already being impacted. Also, the litigants flesh out these issues — and explain the technology's purpose — in their briefs.

Despite assistance from demonstrated use and from litigants' briefs, it is impossible for Justices to escape the difficulties that come along with speedy technological development. How are the Justices

---

88. Grabowski acknowledges this fact later in his article when discussing how Justices could learn to use technology, yet does not mention it as a mitigating factor for many of the potential problems he discusses, like case selection. *See* Grabowski, *supra* note 74, at 109–10.

89. Of course, using analogies is not always the safest way to deal with developing technology. *See* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U.L.J. 475, 477 (2012).

90. SCIENCE FOR ALL AMERICANS ONLINE, *Chapter 3: The Nature of Technology*, *available at* http://www.project2061.org/publications/sfaa/online/chap3.htm (last visited May 9, 2015).

91. *See* David J. Farber, Predicting the Unpredictable — Technology and Society (unpublished manuscript), *available at* http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/farber.pdf; *see also* Nathan Rosenberg, *Uncertainty and Technological Change*, 40 FED. RES. BANK OF BOS. (1996), *available at* https://www.bostonfed.org/economic/conf/conf40/conf40d.pdf (arguing that the future impact of successful innovation has historically been predicted poorly).

meant to interpret the law in a technology-neutral way, that is, create rules that can be applied to as-yet-unforeseen inventions? Such a feat may not be possible, which illuminates another strength of the rules the Court has articulated: They are narrow and do not attempt to regulate technology that does not yet exist, or they regulate existing technology by imagining ways in which it is not being used.

For example, the Court declined to address whether the *use* of the GPS device in *Jones* — continuous surveillance for four weeks to track each location Jones visited — violated a reasonable expectation of privacy, and instead decided it based on the *installation*.[92] This leaves open the question of the reasonableness of long-term GPS tracking, but, as Justice Sotomayor pointed out in her concurrence, trespass "supplies a narrower basis for decision."[93] The ruling also left open whether tracking with existing GPS devices — with which all modern cell phones and most vehicles are equipped — requires a warrant.[94] However, this is not the type of surveillance the Court is seeing — yet.

While it may seem counterintuitive that frequent litigation is the best thing for this area of law, American citizens deserve to challenge new investigative technology as it becomes, as many predict, more and more intrusive.

C. Administrability for Law Enforcement

"Vagueness turns the law into a sword dangling over citizens' heads."[95] Stay out of the home. Do not physically trespass on anything but open fields. These are easy rules for law enforcement to follow, and this clarity is a great strength. Indeed, not all constitutional holdings are so clear, leaving law enforcement to decide for themselves, on the fly, what is acceptable practice.

The Court has recognized the danger of vagueness, and has struck down state laws under the vagueness doctrine. In *Chicago v. Morales*,[96] the Court struck down a law that banned criminal street gang members from loitering with other people in a public space; six members of the Court decided that the ordinance was too vague because it failed to provide minimal guidelines to control police discretion when

92. United States v. Jones, 132 S. Ct. 945, 953 (2012).

93. *Id.* at 957 (Sotomayor, J., concurring).

94. Mike Masnick, *Fourth Amendment Lives? Supreme Court Says GPS Monitoring Is a Search that May Require Warrant*, TECHDIRT (Jan. 23, 2012), http://www.techdirt.com/articles/20120123/11261317515/fourth-amendment-lives-supreme-court-says-gps-monitoring-is-search-that-may-require-warrant-updated.shtml.

95. Timothy Sandefur, *Get Rid of Vague Laws*, FORBES (Mar. 30, 2010), http://www.forbes.com/2010/03/30/vague-laws-economy-government-opinions-contributors-timothy-sandefur.html.

96. 527 U.S. 41 (1999).

enforcing the law.[97] Before 2001, the Court had not made much effort to clarify search and seizure rules, resulting in "a paradox in the Court's thinking: The Court [was] clearly of two minds regarding the Constitution's tolerance for police discretion. Despite an explicit reference in the Constitution's text that limits governmental intrusions, the Court's Fourth Amendment cases regularly allow[ed] police broad discretion in conducting searches and seizures."[98] Shortly before the *Morales* decision, the Court decided that police officers could search a woman's purse in a car pulled over for a brake light, despite a lack of evidence that drugs were inside it,[99] and that police have the power to seize a vehicle from a public place when they have probable cause that it is forfeitable contraband, even though the owner was in custody and the police offered no reason for their failure to obtain a warrant.[100]

The Court has extolled the virtues of bright-line rules in other criminal procedure contexts. For example, in *Fare v. Michael C.*, the Court explained that the

> relatively rigid requirement that interrogation must cease upon the accused's request for an attorney . . . has the virtue of informing police and prosecutors with specificity as to what they may do in conducting custodial interrogation, and of informing courts under what circumstances statements obtained during such interrogation are not admissible. This gain in specificity, which benefits the accused and the State alike, has been thought to outweigh the burdens that the decision in *Miranda* imposes on law enforcement agencies and the courts by requiring the suppression of trustworthy and highly probative evidence even though the confession might be voluntary under traditional Fifth Amendment analysis.[101]

Notably, the two rules discussed here were articulated after *Morales*, perhaps reflecting recognition that restraining police discretion in the area of search and seizure is a positive endeavor. First, it promotes "rule of law" values,[102] reducing "evils" such as "caprice and whim, the misuse of government power for private ends, and the unacknowledged reliance on illegitimate criteria of selection," and

---

97. *Id.* at 64.

98. Tracey Maclin, *What Can Fourth Amendment Doctrine Learn from Vagueness Doctrine?*, 3 U. PA. J. CONST. L. 398, 401 (2001).

99. Wyoming v. Houghton, 526 U.S. 295, 307 (1999).

100. Florida v. White, 526 U.S. 559, 561 (1999).

101. 442 U.S. 707, 718 (1979).

102. Maclin, *supra* note 98, at 408.

advances goals like "regularity and evenhandedness in the administration of justice and accountability in the use of government power."[103]

Second, the restraint of police discretion is consistent with the underlying purpose of the Fourth Amendment when it was adopted: "controlling the discretion of government officials to invade the privacy and security of citizens, whether that discretion be directed toward the homes and offices of political dissentients, illegal smugglers, or ordinary criminals."[104]

Third, police restraint is "a superior analytical tool to the Court's reasonableness model"[105]: If instead of reasonableness, controlling police discretion were the touchstone of the Fourth Amendment, "suspicionless police searches and seizures would not be permitted."[106] The reasonableness formula that judges used (and, in many cases, still use) to decide whether an investigation passes constitutional muster "lacks content and amounts to nothing more than an *ad hoc* judgment about the desirability of certain intrusions."[107]

Finally, using police restraint as the touchstone by articulating clear rules might lend Fourth Amendment cases an "identifiable theme," rather than leaving it as an unruly area of law.[108]

V. THE RULES' LIMITATIONS

The rules are clear, but they do not cover every situation that arises pertaining to the Fourth Amendment and technology. When the rules do not apply, courts return to *Katz*'s reasonable expectation of privacy standard — not always an easy one to apply to new settings. The Court misapplied its standards to DNA evidence in *Maryland v. King* and is likely to run into issues facing encryption and private communications conducted in public places.

A. DNA Typing

The Court's dealings with DNA evidence have betrayed an unfortunate befuddlement as to how to analyze technology. A 2013 case illuminates the danger of drawing a reductive analogy, and what can happen when the Court attempts to make decisions based on technical, rather than capability-based, analysis of technology.

---

103. John Calvin Jeffries, Jr., *Legality, Vagueness, and the Construction of Penal Statutes*, 71 VA. L. REV. 189, 212 (1985).

104. Tracey Maclin, *Informants and the Fourth Amendment*, 74 WASH. U.L.Q. 573, 585 n.53 (1996).

105. Maclin, *supra* note 98, at 415.

106. *Id.* at 416.

107. *Id.* at 419.

108. *Id.* at 416.

In *Maryland v. King*,[109] the petitioner Alonzo Jay King, Jr. challenged Maryland's DNA Collection Act (the Act), which authorizes law enforcement to collect DNA cheek swabs from anyone arrested and charged with "a crime of violence or an attempt to commit a crime of violence . . . or burglary or an attempt to commit burglary."[110] King claimed that the DNA swab was an unreasonable search in violation of the Fourth Amendment because he had a reasonable expectation of privacy in his DNA typing.[111]

The DNA evidence was collected upon arrest but would not be entered into any database until arraignment, when a judicial officer had ensured that there was probable cause to detain King on a qualifying serious offense. If it had been determined that probable cause was lacking, or if the criminal action had not resulted in conviction or ended in reversal or pardon, the sample would have been destroyed.[112] The use of the DNA evidence was also limited — it could be used only for identification purposes.[113]

Justice Kennedy immediately recognized the importance of the technology at issue here: "The advent of DNA technology is one of the most significant scientific advancements of our era."[114] He also stated that the swab constitutes a search under the law, so the Fourth Amendment applied.[115] Thus the question in *King* was whether the warrantless search is reasonable in its scope and manner of execution.[116]

The Court held that it was. The Court emphasized the need for law enforcement to know "who has been arrested and who is being tried";[117] the government has a significant interest in the identification function of DNA evidence since arrestees can conceal their identities.[118] Moreover, the Court said that a suspect's criminal history is a part of his identity that officers should know, since "[p]eople detained for minor offenses can turn out to be the most devious and dangerous criminals."[119] Justice Kennedy compared DNA analysis as a tool for identification to fingerprint databases, booking photograph comparisons, and tattoo matching — a match in the DNA database to a past crime is similar to "common practice."[120] Knowing the true identifica-

109. 133 S. Ct. 1958, 1965 (2013).
110. MD. PUB. SAF. CODE ANN. § 2-504(a)(3)(i)(1)–(2) (Lexis 2014).
111. *King*, 133 S. Ct. at 1966.
112. *Id.* at 1967.
113. *Id.*
114. *Id.* at 1966.
115. *Id.* at 1969.
116. *See id.* at 1970.
117. *Id.* at 1971 (quoting Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cnty., 542 U.S. 177, 191 (2004)).
118. *See id.* at 1977.
119. *Id.* at 1971 (quoting Florence v. Bd. of Chosen Freeholders of Cnty. of Burlington, 132 S. Ct. 1510, 1520 (2012)).
120. *Id.* at 1971–72.

tion (ostensibly the true dangerousness) of an arrestee also allows officers "to make critical choices about how to proceed"[121] and helps courts ensure arrestees' availability for trial and make bail determinations.[122] Finally, a DNA match to a past crime can free an innocent person serving time for that offense.[123]

Justice Kennedy placed much weight on the analogy between fingerprinting and DNA testing.[124] Fingerprinting, he noted, does not violate the Fourth Amendment since it fits within legitimate identification purposes and is therefore "a natural part of the administrative steps incident to arrest."[125]

Conceding that "a significant government interest does not alone suffice to justify a search,"[126] Justice Kennedy then turned to the question of whether a person has a legitimate expectation of privacy in their identification by DNA analysis. Since the person at issue had been arrested with probable cause for serious offenses, he had a reduced expectation of privacy; a relatively non-intrusive cheek swab is therefore reasonable.[127] Moreover, the safeguards built into the Act guard against further invasion of privacy.[128]

Since the question in this case was whether the search involved was reasonable, rather than whether the practice was a search at all, the articulated rules from Part III do not apply here. Nevertheless, what can be said is that the Court applied its general principles on technology — the ones that appeared to guide its rulings in *Kyllo* and *Jones* — incorrectly here.

The Court engages in an inaccurate assessment of the mechanics and capabilities in this opinion. As explored in Part IV.A, *supra*, the Court need only understand and explore the capabilities of technology — not the actual scientific mechanics of how the technology works. However, here, the Court took the mechanics of DNA and, instead of exploring the constitutionality of actual capabilities, it held on to one mechanical capability and merely relabeled all others (as "identification") so that they sounded like something unarguably constitutional: fingerprinting. The analogy is misplaced, as Justice Scalia explained at length in his dissent. The use of fingerprints differs vastly from the use of DNA — fingerprints are taken to identify arrestees while DNA is taken solely to solve crimes.[129] Instead of acknowledging this difference, Justice Kennedy looked at the mechanics of the

121. *Id.* at 1972.
122. *Id.* at 1973.
123. *Id.* at 1974.
124. *See id.* at 1976 ("Perhaps the most direct historical analogue to the DNA technology used to identify respondent is the familiar practice of fingerprinting arrestees.").
125. *See id.* (internal quotation marks omitted).
126. *Id*. at 1977.
127. *Id.* at 1977–78, 1980.
128. *Id.* at 1979.
129. *Id.* at 1987 (Scalia, J., dissenting).

technology to deduce that DNA is used for identification purposes. He chose to stick to that one capability, instead of recognizing the constitutional significance of the other capabilities — what the technology is actually used for; rather than simple identification for identification's sake, it is used to link people to unsolved crimes.[130] He devoted much of the opinion to exploring this capability, yet still lumped it in with the category of identification. It is a vast expansion of the term "identity" to include associations with past crimes for which a detainee has not been arrested — a point Justice Scalia made in his dissent.[131] That DNA is ripe for abuses beyond even the crime-solving use is also problematic.[132]

Instead of engaging in this challenging discourse (which may well have resulted in a holding that DNA collection upon arrest is not acceptable), the Court ignored actual practice and made a broad ruling that "diminish[es] the interest in genetic privacy altogether."[133] Whether the Court was misunderstanding the technology or engaging in definitional gymnastics for crime-solving purposes, it assessed "reasonable expectation of privacy" the wrong way, which may have far-reaching consequences for civil liberties.[134]

B. Encryption

Encryption technology challenges the traditional conception of a reasonable expectation of privacy. In general, the Court has held that one does not have a reasonable expectation of privacy in any data disclosed to a third party.[135] This third party rule, like the two rules discussed in this Note, is a rather clear one and has yet to be

130. *See id.* at 1971.

131. *Id.* at 1982–83 (Scalia, J., dissenting) ("If identifying someone means finding out what unsolved crimes he has committed, then identification is indistinguishable from the ordinary law-enforcement aims that have never been thought to justify a suspicionless search."). Indeed, as Justice Scalia pointed out, King's DNA sample was not used to identify who he was; the sample was not tested for months after his arrest, and when a match came back, it was with the previously-taken sample from an earlier crime. *Id.* at 1983–85.

132. Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161, 178 (2013).

133. *Id.* at 174. The Court insists that DNA typing is a "brief" and "minimal intrusion." *See King*, 133 S. Ct. at 1979.

134. *See King*, 133 S. Ct. at 1989 (Scalia, J., dissenting) ("Make no mistake about it: As an entirely predictable consequence of today's decision, your DNA can be taken and entered into a national DNA database if you are ever arrested, rightly or wrongly, and for whatever reason.").

135. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442 (1976) (finding no reasonable expectation of privacy in bank records since they are provided to the bank); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding no reasonable expectation of privacy in data accessed by pen register, since such data was provided to telephone company).

overturned.[136] It has been applied to all banking activity, phone data, and, most jarringly, e-mails,[137] since all such data is passed to a third party at some point. Encryption, however, complicates the analysis: Once encrypted, an Internet communication is practically impossible to decrypt by guessing — such a process would "occupy a supercomputer for millions of years."[138] Therefore, converting ciphertext (encrypted text) into plaintext (readable text) requires an encryption key. This purposeful cryptography and the impossibility of decryption, according to some Internet law scholars, create a reasonable expectation of privacy in the communication.[139] These scholars analogize the "locked" data to a locked box, in which one has an unquestioned expectation of privacy.[140] As such, "any regulatory scheme that allows the government to obtain a user's key and decrypt the communication without a warrant," or any attempts to decrypt without a warrant, "would violate the Fourth Amendment."[141]

Those who disagree argue that the Fourth Amendment regulates government *access* to communications, not the *cognitive understanding* of communications already obtained. Orin Kerr argues that the "lock and key" analogy is inappropriate for encrypted documents, since a physical lock prevents one from gaining access to the container's contents, while encryption merely makes something unreadable — the contents have already been accessed, and the only thing in the way of comprehension is cognitive discovery, which nobody has a right to stop.[142] "Once ciphertext is in plain view, the communication itself is in plain view for Fourth Amendment purposes."[143] As such, "[w]henever the government obtains ciphertext consistently with Fourth Amendment standards, decrypting the communication into plaintext without a warrant cannot violate the Fourth Amendment."[144] Indeed, if one analogizes encrypted data to general secret communications, rather than locked boxes, the case for protection does not look

136. *Cf. Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (expressing that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties").

137. Whether there is a reasonable expectation of privacy in e-mails or other information provided to Internet service providers ("ISPs") has only been addressed by lower courts — not yet in the Supreme Court. *See, e.g.*, United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999) (finding no expectation of privacy in personal information supplied to an ISP); Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001) (no expectation of privacy in Internet bulletin board subscriber information because the user revealed it to a third party). *But see* United States v. Warshak, 631 F.3d 266, 286–88 (6th Cir. 2010) (finding reasonable expectation of privacy in e-mails through analogy to traditional mail, which is protected by the Fourth Amendment).

138. Kerr, *supra* note 18, at 503.

139. *Id.* at 504.

140. *Id.*

141. *Id.*

142. *Id.* at 521–22.

143. *Id.* at 505.

144. *Id.*

so good. While the Supreme Court has refrained from making any rulings on this subject, lower courts have ruled on the issue. For instance, the First Circuit held, in *United States v. Scott*,[145] that shredding documents before disposing of them does not create a legitimate expectation of privacy. In explaining its decision, the court referenced codes:

> A person who prepares incriminatory documents in a secret code . . . and thereafter blithely discards them as trash, relying on the premise or hope that they will not be deciphered . . . by the authorities could well be in for an unpleasant surprise if his code is "broken" by the police . . . but he cannot make a valid claim that his subjective expectation in keeping the contents private by use of the secret code . . . was reasonable in a constitutional sense.[146]

Similarly, the Tenth Circuit, in *United States v. Longoria*,[147] decided that encoding communications in a foreign language does not create Fourth Amendment protection, and the Pennsylvania Supreme Court held in *Commonwealth v. Copenhefer*[148] that deletion of files (which did not actually delete them) does not create an expectation of privacy. Since all of this evidence was validly seized, the courts held that the government was permitted to analyze and manipulate it.[149] Based on these cases, it seems that the Fourth Amendment does not prevent the government from devoting its resources to decrypting any seized encrypted communications — though, of course, it is likely that the government will fail.[150]

More recently, the issue has gotten even more complicated for law enforcement. In September 2014, Apple and Google announced plans to encrypt certain phone information by default on new versions of their mobile operating systems. This meant that this information is no longer obtainable by those companies — and, in turn, no longer obtainable by law enforcement, even if armed with a valid warrant.[151] Apple wrote on its website, "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government war-

145. 975 F.2d 927 (1st Cir. 1992).
146. *Id.* at 930.
147. 177 F.3d 1179, 1183 (10th Cir. 1999).
148. 587 A.2d 1353, 1356 (Pa. 1991).
149. *Id.* at 1356.
150. Kerr, *supra* note 18, at 517–18.
151. Mike Masnick, *Law Enforcement Freaks Out over Apple & Google's Decision To Encrypt Phone Info by Default*, TECHDIRT (Sept. 23, 2014), https://www.techdirt.com/articles/20140923/07120428605/law-enforcement-freaks-out-over-apple-googles-decision-to-encrypt-phone-info-default.shtml.

rants for the extraction of this data from devices in their possession running iOS 8."[152] This development came just five months after the Supreme Court held in *Riley v. California*[153] that police need a search warrant to collect information stored on phones. Apple's encryption plans (and similarly, Google's) made "that distinction largely moot by depriving itself of the power to comply with search warrants for the contents of many of the phones it sells."[154]

The verbal backlash from the government was immediate and strong. Ronald T. Hosko, the former head of the FBI's criminal investigative division, claimed that increased prevalence of encryption will undermine the government's ability to conduct legal surveillance.[155] One Justice Department official likened the encryption default to giving customers "the equivalent of a house that can't be searched, or a car trunk that could never be opened."[156] Andrew Weissman, a former FBI general counsel, stated that Apple was "announcing to criminals, 'use this.'"[157]

The Court has yet to address this issue, but its two articulated rules — about the home and physical trespass — will not assist it when it inevitably does.[158] Instead, it will have to balance citizens' privacy rights with the well-articulated interest of somewhat simpler enforcement of laws. This balance will lead the Court either to the government's selected analogy — that encrypted information is like secret communication — or the alternative — that encryption is like a locked box, in which citizens have a reasonable expectation of privacy.

Perhaps the Court will chart a new course in recognition that encryption is unlike anything that precedent has seen before. After all, analogies are not always helpful, especially as applied to new technology; many are flawed since they do not "comport with the actual expectations of today's society, expectations that are shaped by factors not present in the pre-digital era."[159] Cass Sunstein, in his article *On*

---

152. *Privacy — Government Information Requests*, APPLE, https://www.apple.com/privacy/government-information-requests (last visited May 9, 2015).

153. 134 S. Ct. 2473 (2014).

154. Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

155. *Id.*

156. Devlin Barrett & Danny Yadron, *U.S. News: Phone Protections Alarm Law Enforcement — Moves by Apple and Google To Put Some Data out of Reach of Police Are Latest Fallout from Snowden's Disclosures*, WALL ST. J., Sept. 23, 2014 at A1.

157. *Id.*

158. More and more Internet companies are utilizing encryption in an effort to safeguard users' data. Apple's iMessage service is the most popular usage of encryption to date. *See* Scott Henson, *Encryption for Cloud Communications May Best Protect Fourth Amendment Rights*, GRITS FOR BREAKFAST (Apr. 6, 2013), http://gritsforbreakfast.blogspot.com/2013/04/encryption-for-cloud-communications-may.html.

159. McAllister, *supra* note 89, at 480.

Analogical Reasoning, recognizes "that analogical reasoning does not guarantee good outcomes or truth."[160] In cases that implicate emerging technologies, "courts often resort to easy analogies without truly analyzing the precise question presented: whether the defendant's particular expectation of privacy is one today's society recognizes as reasonable."[161] Analogy alone cannot reveal the answers in these cases, or else "actual expectations of privacy would be irrelevant to the analysis."[162] Indeed, the Court decided *Jones* by analogizing cars to "effects," such that the placement of the GPS device was rendered a trespass and therefore a search.[163] However, five of the Justices considered the length of surveillance as a critical factor, along with the invasive nature of tracking a target's every move[164] — factors that fit better in the fact-based *Katz* analysis.

A citizen's choice to encrypt her information shows an intention to make that information private, demonstrating at the very least a subjective expectation of privacy. That encryption of data and therefore increased privacy protections is nowadays cast as a competitive edge demonstrates that consumers believe their privacy is important, making it all the more likely that this expectation of privacy is one that society is willing to recognize as reasonable. As such, if the Court chooses to apply *Katz*, rather than limited analogies, encryption should prevail.

C. Private Communications in Public Places

Before high-powered microphones and other "sense-enhancing" technologies were available to the government, there was little to no concern about an expectation of privacy in conversations — in private *and* public spaces. That right to privacy was not explicitly protected, but those exchanges were functionally private. Now, remote or high-powered microphones can pick up sound from great distances, making "private" conversations in public places ripe for the taking. The Court's articulated rules, forbidding physical trespass upon private property and gathering data from the inside of a home, clearly do not apply to information gathered from public places. So, as in most other

160. Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741, 745 (1993).

161. McAllister, *supra* note 89, at 483–84 (emphasis omitted).

162. *Id.* at 484.

163. *See* United States v. Jones, 132 S. Ct. 945 (2012).

164. *Id.* at 955–56 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . . I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."); *id.* at 964 (Alito, J., concurring) (finding the "lengthy" monitoring of Jones a search because "the line [between an acceptable length of time and an unacceptable length of time] was surely crossed before the 4-week mark").

settings that do not fit the rules, *Katz*'s reasonable expectation of privacy test might remain the standard.

How this issue will be decided is unclear. On the one hand, the Court has said that one cannot have a reasonable expectation of privacy in what one exposes to the public.[165] It is possible, then, that technology will not change this seemingly bright-line rule. However, the Court in *Katz* offered that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[166] The Court pointed out that Katz entered a phone booth, shut the door behind him, and paid a toll so that he could place a call — acts that "surely entitled [him] to assume that the words he utters into the mouthpiece will not be broadcast to the world."[167] The Court has given Fourth Amendment protection to people in a business office,[168] a friend's apartment,[169] and a taxicab[170] — but each of these locations involves a closed door. The Court has not yet ruled that the affirmative act of closing a door is the factor upon which a reasonable expectation of privacy turns.

The mosaic theory of the Fourth Amendment could also apply here. In *Jones*,[171] five Justices authored or joined concurring opinions that applied a new approach to assessing whether government activity constituted a search; rather than evaluating each step of an investigation in isolation, a court should look at all of the steps as one whole to consider whether the sequence is a search.[172]

Applied to the expectation of privacy in public conversations context, it is reasonable to suggest that where a person goes in a car should be like what a person says on a street. Monitoring someone's movements on public streets on its own typically does not constitute a search, much like overhearing someone's conversations — however, when combined with new technology, it may be enough to violate a reasonable expectation of privacy.

There is reason to believe that this theory is gaining traction. On December 16, 2013, Judge Leon of the United States District Court for the District of Columbia ruled, in a strongly worded opinion, that the National Security Agency's program that gathers telephone call

---

165. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

166. *Id.* at 351–52.

167. *Id.* at 352.

168. Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920).

169. Jones v. United States, 362 U.S. 257 (1960).

170. Rios v. United States, 364 U.S. 253 (1960).

171. The mosaic theory was initially introduced by the D.C. Circuit in its consideration of *Jones*, in United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

172. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012).

metadata constitutes a search — likely an unconstitutional one.[173] Though the decision has been critiqued as "tr[ying] to anticipate where the justices might be heading based on concurring rather than controlling opinions,"[174] the law may very well be headed in this direction and discussions in public places could gain protection because of it.

VI. CONCLUSION

Technology complicates Fourth Amendment analysis by challenging what is "reasonable" about privacy. Faced with new situations and enhanced surveillance measures, the Supreme Court has proceeded cautiously — and writing clear and narrow holdings has its own strengths. Unfortunately, some new situations simply do not fall within the Court's bright-line rules; for these, the Court will rely either on the abstract "reasonable expectation of privacy" test, or craft something entirely new. While rules like the ones the Court has already articulated practically guarantee further litigation about similar situations, continued litigation in this area of law and articulation of more sensible rules is important, if not necessary, to preserving the rights of Americans.

173. Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013) ("Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware 'the abridgement of freedom of the people by gradual and silent encroachments by those in power,' would be aghast.").

174. Adam Liptak, *After Ruling Critical of N.S.A., Uncertain Terrain for Appeal*, N.Y. TIMES (Dec. 17, 2013), http://www.nytimes.com/2013/12/18/us/politics/after-ruling-critical-of-nsa-uncertain-terrain-for-appeal.html?pagewanted=1&hp&_r=0.