TELEPHONES, AERIAL SURVEILLANCE, AND PRIVACY RIGHTS

By Matthew Henshon

Fourth Amendment privacy jurisprudence would seem to be a highly specialized purview of criminal defense lawyers. However, it also offers a prism to examine how the Supreme Court's view of privacy has evolved in the face of advancing technology. The language of the Fourth Amendment has not changed in 200 years, but the Court's interpretation of it has.[1] And tracking Fourth Amendment jurisprudence over the last century provides an interesting roadmap to think about how rule makers (i.e., judges, legislators, and, in some cases, private parties) have thought—and likely will think—about the right to privacy in the context of UAVs and other advanced technologies.

A century ago, one of the most advanced technologies was the telephone, which was invented in 1876 by Alexander Graham Bell, and by the early 20th century was in wide use. Accordingly, the use of a phone soon became a target for law enforcement. In *Olmstead v. United States*,[2] and focusing on the physical description of "houses" in the text of the Amendment, the Supreme Court found no privacy in the government's tapping of telephone wires in streets outside the house. The Court determined that "the wires beyond his house and messages while passing over them are not . . . [protected]. . . . Here, those who intercepted the projected voices were not in the house of either party to the conversation."[3] Thus, the Court's reasoning was based on place, not rights inherent in the conversation. The telephone wire, once it left the physical domain of the defendant, was fair game.

The *Olmstead* property-line definition of privacy persisted for close to 40 years, even as technology advanced, such as the widespread distribution of public telephones—booths that were in public places. In *Katz v. United States*,[4] the government intercepted a phone call made from a public phone booth in the Los Angeles railway terminal at Union Station. But the Court deemed the phone call to be private—the government's interception of the call was considered an unreasonable infringement on private affairs. But it is Justice Harlan's concurring opinion that has set the privacy standard going forward: "a twofold requirement, first that a person has exhibited an *actual (subjective) expectation of privacy* and, second, that the expectation be one that society is prepared to recognize as '*reasonable*.'"[5] In shorthand, courts began to search for a "reasonable expectation of privacy."

But the reasoning behind *Katz* is inherently flawed. *Katz*'s view of privacy is that it is determined by the "reasonable expectation" of citizens. Accordingly, if the expectation of privacy changes, so seemingly does the scope of *Katz*'s protection. Observers recognized this problem almost immediately after the *Katz* decision:

> An actual, subjective expectation of privacy . . . can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection. If it could, the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance.[6]

Amsterdam's implication is that privacy could easily be restricted by governmental (or other) action. But the opposite is also true—that is, the reasonable expectation of privacy could be increased over time, whether through other constitutional cases, legislation, or market forces.

For example, just two years before *Katz* was decided, the Supreme Court identified a (previously unarticulated) "right to marital privacy" in *Griswold v. Connecticut*.[7] Although *Griswold* was not decided exclusively on Fourth Amendment grounds, the Court cited the "penumbras, formed by emanations" from a number of articles in the Bill of Rights, including the Fourth Amendment.[8] Just six years after *Katz*, the Court further expanded privacy in *Roe v. Wade*,[9] and has subsequently further expanded similar rights via *Obergefell v. Hodges*,[10] which permitted same-sex marriages. Regardless of what one thinks of the jurisprudence—or the Court's future views—of the *Griswold/Roe/Obergefell* line of cases, the expansion of "privacy" in the personal realm occurred.

Legislation can also have impacts on reasonable expectations of privacy. For instance, many citizens have expressed concern about protecting their interactions in the public sphere—in particular, the privacy of borrowing records from public libraries. (Interestingly, the borrowing of any single particular book is effectively a public event—it could easily be observed by anyone standing in proximity to the checkout counter when the book is borrowed.[11]) States just as diverse as Maine,[12] Alaska,[13] and Arizona[14] have limited—or otherwise regulated—the availability of borrowing records, effectively "creating" a right of privacy in that area.

The market, too, can have an influence on reasonable expectations of privacy. For instance, in July 2012, the *New York Times* found it was worth reporting that your phone could also serve as a step or mileage tracker.[15] But within three years, Apple had added a feature that allowed the tracking function to be disabled, and the paper explained how to do so.[16]

At least three cases in the post-*Katz* era have relevance to the use of UAVs by law enforcement and/or others. In *California v. Ciraolo*,[17] a plane flew at 1,000 feet and allowed a police officer to observe marijuana plants being grown in a backyard. The Court's ruling stated, "The . . . observations . . . took place within public navigable airspace, in a physically nonintrusive manner."[18] Accordingly, there was a finding of no expectation of privacy. Similarly—and decided the same year as *Ciraolo*—*Dow Chemical Co. v. United States* found that the EPA could utilize commercial photographs taken from as a low as 1,200 feet above a chemical plant that was otherwise fenced off.[19]

A few years later, the Court again reviewed aerial observation of marijuana plants in *Florida v Riley*.[20] This time, however, the helicopter was hovering at 400 feet. Unlike *Ciraolo*, which was decided 5 to 4, the Court was only able to reach a plurality upholding the constitutionality of the search. Justice O'Connor, who was the deciding vote, commented

that "compliance with FAA regulations alone"[21] should not be the determinate of reasonable expectations of privacy. But it was Justice Brennan's dissent that pointed to the future, writing:

> The vantage point . . . was not one any citizen could readily share. [The] ability to see over Riley's fence depended on [the] use of a very expensive and sophisticated piece of machinery to which few ordinary citizens have access.[22]

But it was *Kyllo v. United States*[23] where the Court's reasonable-expectation doctrine ran into the problem of how fast technology was changing and being adapted. In *Kyllo*, the government was again concerned with the growth of marijuana—but this time it was observed from ground level. Law enforcement in *Kyllo* used a thermal imager to determine that heat lamps were being utilized to grow illicit plants; but here the Court drew a line, stating that use of a "device that is not in general public use, to explore details of a private home that would previously have been unknowable . . . is . . . presumptively unreasonable."[24]

With *Kyllo*, the Court now recognized that the reasonable expectations of privacy change over time as technology changes. Six years after *Kyllo*, Apple had introduced the iPhone. While the connection between smartphones and UAVs may not be obvious, here's what one pioneer in the drone space observed:

> I had the fortune of getting into this business in 2007, the year the iPhone was released, and so, as a result, everything we did was oriented around smartphone architectures, and inherited everything smartphones have—connectivity; sensors; an incredible, Moore's Law pace of processing. But by doing that, we inherited the architecture of the cloud as well—smartphones are a connected device. The old world—the aerospace world—thought of [airborne] vehicles as being a stand-alone category, with their own intelligence. But we thought of drones as being smartphones with propellers.[25]

The price of a drone is trending down, while the functionality of the average drone is trending up. As drone use becomes more prevalent, legal challenges to the ability of users—both law enforcement and private parties—will increase. It will not be long before they are considered (in Justice Scalia's words from *Kyllo*) "in general public use"—if we have not reached that point already. And the Court will have to try and define these limits.

The Court may be recognizing the problem of technological advance.[26] In 2012, the Court again revisited the effect of technology on Fourth Amendment searches; in *Riley v. California*,[27] a unanimous Court determined that warrantless search of the contents of a cell phone's memory was unconstitutional. Chief Justice Roberts wrote:

> Digital 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. . . . Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one. . . . Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life."[28]

Finally, the Court recently reviewed the protection of cell phone records held by third parties (i.e., the cell phone companies). While the tracking of cell phones (by where the phone "pings" off cell phone towers) is "public"—in the sense that it was available to the cell phone operator—without a warrant, the records could allow the government to have "near perfect surveillance" of an individual's movements.[29] Chief Justice Roberts went on to observe:

> Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in [previous cases involving third-party information] and the exhaustive chronicle of location information casually collected by wireless carriers today.[30]

The reality that the Court is grappling with is that changes in technology change our view of the "reasonable expectation of privacy" over time. For instance, telephones were originally party lines (especially in rural areas) that allowed anyone in the same neighborhood to listen in on a "private" conversation. Likewise, even after fixed landlines were established in each home or office, an operator had to physically connect calls by plugging in a line to a connector in a telephone office.[31] In the modern era, the perhaps watershed moment came when TiVo reported that Janet Jackson's "wardrobe malfunction" at the Super Bowl in 2004 had become the biggest "reviewable" moment in TiVo history.[32]

As drone technology becomes more prevalent, and smartphones continue to add additional features, "reasonable expectations" will be subject to adjustment. On the one hand, users of technology understand that their digital footprint is becoming sharper and easier to track. Yet, at the same time, we understand that allowing Big Tech—and, by extension, the government—access to all that information makes us uncomfortable.

In Europe, privacy has been defined by a "right to be forgotten," which can play out over decades.[33] For instance, in 1998, the Spanish paper *La Vanguardia* published notices about an auction of the property of an indebted lawyer. More than a decade later, the lawyer asked Spanish courts to force newspapers to take down notices and also remove Google's applicable links. In 2014, European Court of Justice agreed, forcing Google to shut down links.[34] The EU has subsequently

passed the General Data Protection Regulation (GDPR), which is more expansive than the previous law.[35]

In recent years, California's expansive Consumer Privacy Act of 2018 (CCPA) broke new ground in consumer privacy protection. But in November 2020, the California electorate passed Prop[osition] 24, known as the California Privacy Rights Act (CPRA). Although it will not take effect until January 1, 2023, the CPRA will undoubtedly expand "reasonable expectations"—at least for California citizens—with expansions of privacy rights and the creation of a new state privacy enforcement agency to enforce its provisions.[36]

But as technology surges forward, perhaps we should look to the past. In 1890, just a few short years after the invention of the telephone—and before the invention of the airplane—Samuel Warren and Louis Brandeis co-wrote "The Right to Privacy."[37] Citing then-modern advances like "[i]nstantaneous photographs" and "numerous mechanical devices," the two men predicted a new century where "'what is whispered in the closet shall be proclaimed from the house-tops.'"[38] But the co-authors focused on a single right: that to be "let alone." Future courts—and future lawmakers—will likely be struggling with that definition into the 22nd century.[39]

Matthew Henshon is a partner in the boutique Boston firm of Henshon Klein LLP. His practice encompasses a wide range of issues affecting corporations, including governance, intellectual property and technology licensing, and mergers and acquisitions, and his experience includes representation of all sides of the privately held, emerging company: founders, investors, and employees.

ENDNOTES

1. The Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV (1791).

2. Olmstead v. United States, 277 U.S. 438 (1928).

3. *Id.* at 466.

4. 389 U.S. 347 (1967).

5. *Id.* at 361 (emphasis added).

6. Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 59 Minn. L. Rev. 349, 384 (1974).

7. 381 U.S. 479 (1965).

8. *Id.* at 484–85. The Court also made reference to the First, Third, and Fifth Amendments in support of the "penumbras."

9. 410 U.S. 113 (1973).

10. 576 U.S. 644 (2015).

11. *Cf.* California v. Greenwood, 486 U.S. 35 (1988) (allowing inspection of garbage bags placed on the public street just prior to collection without a warrant): "readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.* at 40.

12. Me. Rev. Stat. Ann. tit. 27, § 121 (West 2015).

13. Alaska Stat. § 40.25.140.

14. Ariz. Rev. Stat. § 41-1354.

15. Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker.*, N.Y. Times (July 15, 2012), https://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html.

16. J. D. Biersdorfer, *Stopping the iPhone Step Counter*, N.Y. Times (Aug 12, 2015), https://www.nytimes.com/2015/08/13/technology/personaltech/stopping-the-iphone-step-counter.html.

17. 476 U.S. 207 (1986).

18. *Id.*

19. 476 U.S. 227 (1986).

20. 488 U.S. 445 (1989).

21. *Id.* at 453 (O'Connor, J., concurring). Four hundred feet is the FAA's usual lower limit for manned aircraft not descending to land; Relatedly, the FAA's current regulations (Part 107) for small drones limit their flight to not more than 400 feet. News Release, Fed. Aviation Admin., Fact Sheet—Small Unmanned Aircraft Systems (UAS) Regulations (Part 107) (Oct. 6, 2020), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615#:~:text=The%20maximum%20allowable%20altitude%20is,or%20controllability%20of%20the%20aircraft.

22. *Riley*, 488 U.S. at 460 (Brennan, J., dissenting).

23. 533 U.S. 27 (2001).

24. *Id.* at 40.

25. Chris Anderson, President, 3D Robotics, InterDrone 2016 Keynote Address: Drones and the Future of Cloud Robotics (Sept. 8, 2016), https://www.youtube.com/watch?v=t7qskPaX6Fc, beginning at 0:50.

26. There was the interim case of *United States v. Jones*, 565 U.S. 400 (2012), where the Court found that after a warrant for a GPS device to be attached to a car had expired, further surveillance was improper. But the Court (with Justice Scalia writing) found on common-law trespass grounds—in some ways a callback to *Olmstead.*

27. 573 U.S. 373 (2014).

28. *Id.* at 387, 403.

29. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

30. *Id.* at 2219.

31. For example, the switchboard at the U.S. Capitol grew from 51 to more than 1,200 connections. Harris & Ewing, *First Capitol Telephone Operator Still on the Job. Washington, D.C., July 30 [1937]* (photograph), https://www.loc.gov/item/2016872097.

32. Hugh McIntyre, *How Janet Jackson's Super Bowl "Wardrobe Malfunction" Helped Start YouTube*, Forbes, Feb. 1, 2015.

33. *See* EU Data Protection Directive, officially Directive 95/46/EC.

34. Eric Posner, *We All Have the Right to Be Forgotten*, Slate (May 14, 2014), https://slate.com/news-and-politics/2014/05/the-european-right-to-be-forgotten-is-just-what-the-internet-needs.html.

35. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, which repealed Directive 95/46/EC.

36. Sam Dean, *California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy*, L.A. Times (Nov. 3, 2020), https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24.

37. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

38. *Id.* at 195.

39. For a discussion of the problems inherent in the FAA's ability to protect privacy, see, for example, Melissa Barbee, *Uncharted Territory: The FAA and the Regulation of Privacy Via Rulemaking for Domestic Drones*, 66 Admin. L. Rev. 463–87 (Spring 2014), https://www.jstor.org/stable/24475503.