Privacy in an Era of Advancing Technology

Russell L. Weaver
University of Louisville Louis D. Brandeis School of Law

Follow this and additional works at: https://scholarship.law.ufl.edu/jlpp

Recommended Citation
Available at: https://scholarship.law.ufl.edu/jlpp/vol33/iss2/4

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in University of Florida Journal of Law & Public Policy by an authorized editor of UF Law Scholarship Repository. For more information, please contact rachel@law.ufl.edu.
This Article examines the privacy implications of new technologies, in particular facial recognition technology (FRT), which uses biometric software to recognize a person’s facial features. When used in conjunction with closed-circuit television (CCTV) or drones, FRT has allowed governments to continuously monitor public places and has helped law enforcement officials to locate and apprehend criminals. But many are uneasy regarding the privacy implications of FRT technology, which can often be unreliable. The difficulty is that the Fourth Amendment imposes few meaningful limits on governmental use of modern technologies in public places, although some states have imposed limitations by statute.

INTRODUCTION ..................................................................................... 219

I. THE DEVELOPMENT OF NEWER TECHNOLOGIES ..................... 221

II. THE BENEFITS OF DRONES, FRT, AND CCTV ....................... 222

III. PRIVACY CONCERNS ............................................................... 223

IV. LEGAL LIMITATIONS ................................................................... 225

CONCLUSION ......................................................................................... 233

INTRODUCTION

Technology has made it increasingly difficult for individuals to maintain their privacy. When the United States was founded in the eighteenth century, the government had only crude means for spying on the citizenry. For example, the police might have eavesdropped on their fellow citizens in taverns or other public settings or listened outside a suspect’s window. However, without the advanced technologies that

* Professor of Law and Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law. Professor Weaver wishes to thank the University of Louisville’s Distinguished University Scholar program for supporting his research. Portions of this Article are drawn from a prior publication, Russell L. Weaver, The Constitutional Implications of Drones, Facial Recognition Technology and CCTV, 6 PUB. GOVERNANCE, ADMIN. & FINS. L. REV. 53–65 (2021). Reprinted with permission.

1. See Russell L. Weaver, The Fourth Amendment, Privacy and Advancing Technology, 80 MISS. L.J. 1131, 1136 (2011) (“The steady onslaught of technology has raised troubling implications for individual privacy.”).
exist today, the opportunities for successful eavesdropping were very limited.

The situation is dramatically different today. Surveillance technologies have gone high tech, creating Orwellian possibilities for snooping. As one commentator observed, “rapid technological advances and the consequent recognition of the ‘frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society’ have underlined the possibility of worse horrors yet to come.”

Electricity was a transformative invention because it made possible the creation of super-sensitive microphones with the ability to overhear conversations from far away, as well as through walls, and led to the invention of facial recognition and CCTV systems, which allow the government to maintain continuous surveillance of public places.

Electricity also led to the creation of GPS monitoring systems, which allow the police to monitor the location and movements of individuals and things; X-ray technology, which enables the police to peer through walls and into the privacy of homes by using drive-by X-ray vans; and devices that allow people to monitor the computer key strokes of individuals from distant places.

---


3. See Silverman v. United States, 365 U.S. 505, 506–07 (1961) (demonstrating that advanced surveillance technologies were already available in the 1960s); see also Katz v. United States, 389 U.S. 347, 348 (1967) (involving the attachment of an electronic listening device to the outside of a phone booth so that the police could overhear what was being said inside the phone booth); Goldman v. United States, 316 U.S. 129, 131–32 (1942) (involving the use of a listening device that allowed the police to overhear what was being said in Goldman’s office even though the police were located in an adjoining office); Dina Temple-Raston & Robert Smith, U.S. Eyes U.K.’s Surveillance Cameras, NPR (July 8, 2007, 8:00 AM), http://www.npr.org/templates/story/story.php?storyId=11813693 [https://perma.cc/L4ZN-4FUN] (discussing how police in Great Britain have been using CCTV cameras to combat terrorism since the 1990s).

4. See Devega v. State, 689 S.E.2d 293, 299–300 (Ga. 2010) (finding no violation of the Fourth Amendment when investigators requested that the defendant’s cell phone provider “ping” the defendant’s phone and used GPS to locate the defendant in his vehicle); Andy Greenberg, Scanner Vans Allow Drive-By Snooping, FORBES (Sept. 9, 2010, 12:40 PM), http://www.forbes.com/forbes/2010/0927/technology-x-rays-homeland-security-actu-drive-by-snooping.html?feed=rss_technology [https://perma.cc/J6VB-YQGB] (“American Science & Engineering . . . has sold U.S. and foreign government agencies more than 500 backscatter X-ray scanners mounted in vans that can be driven past neighboring vehicles or cargo containers to snoop into their contents.”); Rania M. Basha, Kyllo v. United States: The Fourth Amendment Triumphs over Technology, 41 BRANDEIS L.J. 939, 939 (2003) (“[T]here are some devices, such as x-ray systems and radar flashlights, which enable officers to see through walls.”); Alan F. Blakley et al., Coddling Spies: Why the Law Doesn’t Adequately Address Computer Spyware, 4 DUKE L. & TECH. REV. 1, 4 n.18 (2005) (explaining the capabilities of spyware, including the monitoring of key strokes). See generally City of Ontario v. Quon, 130 S. Ct. 2619, 2625 (2010) (discussing how a city reserved the right to monitor all network activity on pagers issued to the city’s police); Jason Broberg,
This Article focuses on one of these new technologies: governmental monitoring of citizens in public places through devices such as drones, FRT, and CCTV. As will be seen, in the United States, there are few restrictions on governmental use of these technologies.

I. THE DEVELOPMENT OF NEWER TECHNOLOGIES

U.S. government organizations monitor what happens in public spaces using technologies that only have increased in sophistication and reach over time. By 2018, some 910 state and local public safety agencies, including 599 law enforcement agencies, were using drones.\(^5\) Drones can be equipped with high-powered cameras that allow them to magnify images on the ground by 180 times, thereby making them effective spies that can take detailed pictures of what is happening below.\(^6\) As a result, drones can observe activities that may not be observable from ground level, including things that are happening in individuals’ backyards.\(^7\)

FRT “uses biometric software to map a person’s facial features from a video or photo.”\(^8\) The technology can then identify a person by pinpoint matching his or her facial features with information contained in existing databases.\(^9\) CCTV is also being used to monitor what goes on in public places.\(^10\) For example, in the London Underground, there is a pervasive CCTV system that includes some 15,516 cameras.\(^11\) The United States is

---

6. Id.
7. Id.
9. Id.
awash in CCTV systems, with Atlanta having 15.56 cameras per 1,000 people, and Chicago having 35,000 cameras or 13.06 cameras per 1,000 people. Indeed, six U.S. cities (Atlanta, Chicago, Washington, D.C., San Francisco, San Diego, and Boston) made the list of the most surveilled cities in the world.

II. THE BENEFITS OF DRONES, FRT, AND CCTV

Unquestionably, drones, CCTV, and FRT can offer enormous benefits to governmental officials in their efforts to serve the public. For example, when hikers are lost in remote areas, drones can help locate the hikers. Likewise, following hurricanes, drones can “assess damage, locate victims, and deliver aid.” In an effort to prevent forest fires, drones equipped with thermal imaging cameras can survey forests. Drones can also monitor the health and well-being of wild animals.

CCTV and FRT also are enormously helpful in locating and apprehending criminal suspects. CCTV can provide continuous, recorded video monitoring of public areas, so that the police can review tape recordings and identify suspects after a crime has been committed. Following the London subway bombings in July 2005, during which fifty-two people were killed and another 700 were injured, the bombers were identified through police review of London Underground CCTV footage. Similarly, the Boston Marathon bombers, who killed three people and injured hundreds of others, were found and apprehended using

---


13. Id.


16. Id.

17. Id.

18. See Collins, supra note 8 (“Police departments regularly use facial recognition to find potential crime suspects and witnesses by scanning through millions of photos.”).


CCTV images captured on government and private cameras.21 The bombers stood out on the video because of the way they acted: while the crowd was fleeing the scene, the Tsarnaev brothers lingered around or walked away casually.22 In tracking down those who attacked the U.S. Capitol Building on January 6, 2021, the FBI used CCTV images and FRT, among other techniques.23

III. PRIVACY CONCERNS

As FRT, CCTV, and drones have proliferated, major privacy concerns have arisen. As one writer noted: “[P]rivacy advocates and other citizens are uneasy with the idea that Big Brother is monitoring their every public move.”24 For example, when New York City announced that it was going to deploy fourteen drones, purportedly to assist in emergencies, civil libertarians complained that the drones could “easily be used to track . . . those who speak out against City Hall and police.”25 As one commentator noted, “The NYPD’s drone policy places no meaningful restrictions on police deployment of drones in New York City and opens the door to the police department by building a permanent archive of drone footage of political activity and intimate private behavior visible only from the sky.”26

Similar concerns have been raised regarding FRT. The dimensions of modern FRT are truly staggering:

[W]ith a single high-resolution snap shot, FRT, has the ability to map out a biometric profile that is as individually

21. See Heather Kelly, After Boston: The Pros and Cons of Surveillance Cameras, CNN Bus. (Apr. 26, 2013, 7:03 PM), https://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/index.html [https://perma.cc/A2UX-6R9D] (“After last week’s bombings at the Boston Marathon, authorities had to sift through a mountain of footage from government surveillance cameras, private security cameras and imagery shot by bystanders on smartphones. It took the FBI only three days to release blurry shots of the two suspects, taken by a department store’s cameras.”); see also Role of CCTV Cameras, supra note 19 (“The potential value of public surveillance technology was well demonstrated all the way back in April, 2013 when investigators identified the two suspects in the Boston Marathon bombing after sifting through video images captured by the city’s cameras.”).


24. Kelly, supra note 21.


26. Id.
unique as a human fingerprint. With images sharing the same binary 1 and 0 sequences as text, the source noted that big data software and storage capacity currently exists to construct a truly three-dimensional profile of, well, anyone with a digital image online.27

One source denounced FRT as “an unreliable, biased and dystopian threat to privacy.”28 The American Civil Liberties Union summarized the impact of FRT as follows: “Face recognition offers governments a surveillance capability unlike any other technology in the past. The powerful capability can enable the government to identify who attends protests, political rallies, church, or AA meetings on an unprecedented scale.”29 Despite the concerns, FRT use seems to be expanding and is now used by U.S. Customs and Border Patrol.30

CCTV raises similar concerns. As one commentator argued, “[t]he advent of sophisticated technology that allows the government to watch, zoom in on, track, and record the activities of anyone, anywhere in public, twenty-four hours a day, demands regulation.”31 CCTV is particularly potent when it is combined with FRT. CCTV accumulates a mountain of facial images that can then be fed into an FRT system to identify people.32

The difficulty is that current drones, FRT, and CCTV technology provide only a glimpse of what is to come. The FBI is spending more than a billion dollars to expand its Next Generation Identification (NGI) system.33 That system will include huge amounts of information about

32. See Kelly, supra note 21 ("[F]acial-recognition software and other technologies are making security-camera images more valuable to law enforcement. Now, software can automatically mine surveillance footage for information, such as a specific person’s face, and create a giant searchable database.").
33. See Next Generation Identification (NGI), FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/6HEL-D9SX] (last visited Mar. 29, 2023) ("This new system, the Next Generation Identification (NGI), provides the criminal justice community with the world’s largest and most efficient electronic repository of biometric and criminal history information.").
people, including iris scans, photos, palm prints, gait and voice recordings, scars, tattoos, and DNA.  

IV. LEGAL LIMITATIONS

There are few meaningful limits on governmental use of these modern technologies in public places. There have been isolated attempts by individual jurisdictions to limit or control the use of FRT and CCTV in public spaces. The Electronic Privacy Information Center notes that several U.S. cities (for example, San Francisco, California, Somerville, Massachusetts, and Oakland, California) have banned the use of FRT, and that the State of California has imposed a moratorium on its use. However, there are few restrictions on governmental use of CCTV.

There are some restrictions on government’s use of drones. For example, many states have provisions governing the flying of drones by private citizens, but these laws place few restrictions on governmental use. The federal government does impose some limitations on drone pilots. For example, governmental “pilots” must either comply with Federal Aviation Administration (FAA) Rule 107 waiver requirements or obtain a federal certificate. In addition, drones cannot be flown within


400 feet of the ground or over venues such as military bases or public landmarks.39

One might think that the U.S. Constitution would limit the use of surveillance technologies, but it imposes relatively few restrictions on governmental uses of advanced technologies in public places. The most obvious constitutional limitation is the Fourth Amendment to the U.S. Constitution, which prohibits “unreasonable searches and seizures.”40 Historically, the Fourth Amendment has prohibited only “trespassory” invasions into “constitutionally protected areas.”41 That approach provided few protections against the use of advanced technologies.42 For example, in Olmstead v. United States, when the police wiretapped phone calls made from the defendant’s home, the Court held that there was no “search” within the meaning of the Fourth Amendment because the police did not trespass or intrude into a constitutionally protected area.43 In other words, the wiretapping was permissible because it was conducted from a public place.44 Likewise, in Goldman v. United States, when the police held a “detectaphone” against an office wall, thereby allowing them to overhear what was being said in an adjoining office, the Court again held that there was no search because the police did not trespass into the adjoining office.45

40. U.S. CONST. amend. IV.
41. See, e.g., Goldman v. United States, 316 U.S. 129, 134–35 (1942) (explaining that use of a detectaphone was not an illegal trespass and not a violation of the Fourth Amendment), abrogated by Katz v. United States, 389 U.S. 347, 353 (1967); Olmstead v. United States, 277 U.S. 438, 466 (1928) (“Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house ‘or curtilage’ for the purpose of making a seizure.”), abrogated by Katz v. United States, 389 U.S. 347, 353 (1967); ex parte Jackson, 96 U.S. 727, 733 (1877) (“The constitutional guaranty of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.”).
42. See Weaver, supra note 1, at 1150 (“While the concepts of ‘trespassory invasions’ and ‘intrusions into constitutionally protected areas’ may have made sense as applied to a house, a car or a briefcase, those concepts did not produce satisfactory results as advancing technology provided police investigators with ever more sophisticated surveillance technologies.”).
43. 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.”).
44. Id.
45. Goldman, 316 U.S. at 135. The Goldman Court noted:
It took many decades before the Court started to come to grips with the reality of advancing technologies. The Court’s landmark decision in *Katz v. United States* involved a man who the police suspected was involved in illegal bookmaking operations. The police, anticipating that Katz would make a call from a particular phone booth, placed an electronic bug on the outside of the booth which allowed them to record Katz’s incriminating statements and to use them against him in a subsequent prosecution. Based on decisions like *Olmstead* and *Goldman*, the government argued that the police did not engage in a “search” when they bugged the phone booth since there was no “intrusion” into the phone booth and there was doubt about whether the booth would qualify as a “constitutionally protected area.” The electronic bug placed by the police had done nothing more than passively collect sounds that emanated from a public phone booth.

The *Katz* Court disagreed with the government and held that police use of the listening device to overhear Katz’s conversation constituted a “search” within the meaning of the Fourth Amendment. In reaching that result, *Katz* departed from *Olmstead*’s focus on whether there had been an intrusion into a constitutionally protected area and held that a search occurs when governmental officials violate an individual’s “expectation of privacy” (EOP). In doing so, the Court purported to shift the focus under the Fourth Amendment from places to persons.

The suggested ground of distinction is that the *Olmstead* case dealt with the tapping of telephone wires, and the court adverted to the fact that, in using a telephone, the speaker projects his voice beyond the confines of his home or office and, therefore, assumes the risk that his message may be intercepted. It is urged that where, as in the present case, one talks in his own office, and intends his conversation to be confined within the four walls of the room, he does not intend his voice shall go beyond those walls and it is not to be assumed he takes the risk of someone’s use of a delicate detector in the next room. We think, however, the distinction is too nice for practical application of the Constitutional guarantee and no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the *Olmstead* case.

---

47. *Id.* at 349.
48. *Id.* at 351.
49. *Id.* at 352.
50. *Id.* at 352–53.
51. *See id.* at 353 (“Thus, although a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested.”).
53. *See id.* at 351 (majority opinion) (“For the Fourth Amendment protects people, not places.”).
stated: “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.” Justice Harlan, concurring, agreed with the Court that the focus should be on whether Katz had an EOP, but he argued that the expectation must be one that society was prepared to recognize as “reasonable.” Ultimately, Justice Harlan’s requirement of “reasonableness” was integrated into the EOP test so that the final inquiry became whether the police have intruded upon an individual’s “reasonable expectation of privacy” (REOP).

Thus, after Katz, the Court used two tests to determine whether a “search” occurred under the Fourth Amendment. In addition to the REOP test, the Court continued to apply the old trespass test, which had been the governing test for many decades. For example, in the Court’s later decision in United States v. Jones, the police attached a GPS tracking device to the undercarriage of the defendant’s car. Instead of deciding the case under the Katz test, the Court relied on the trespass test and invalidated the warrantless attachment of the device—and its use to monitor the defendant’s car on public streets.

Unfortunately, in the decades since the Katz test was announced in the 1960s, that test has not provided a workable or reliable test for evaluating Fourth Amendment claims. The REOP test could have led to a

54. Id.
55. See id. at 361 (Harlan, J., concurring) (“As the Court’s opinion states, ‘the Fourth Amendment protects people, not places.’ The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a ‘place.’ 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.’”).
57. Id. at 403, 409.
58. Id. at 406–07. The Jones Court explained, “[F]or most of our history, the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas (‘persons, houses, papers, and effects’) it enumerates. Katz did not repudiate that understanding.” Id. The Court continued, “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.’” Id. at 407 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)). The Court added, “What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide at a minimum the degree of protection it afforded when it was adopted.” Id. at 411 (emphasis in original). Finally, the Court concluded, “[W]e do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis.” Id. (emphasis in original).
59. See Weaver, supra note 1, at 1225 (“The one thing that remains clear, some three decades after the Katz decision was rendered, is that the Court is still struggling to determine what the REOP test means, and there are continuing disputes between the Justices about how to apply the REOP test.”).
significant expansion of the Fourth Amendment’s scope of protection. That is exemplified by *Katz*. In that case, under the trespass test, there would have been no search. Yet, under the REOP test, the Court held that the Fourth Amendment protected an individual who made a phone call from a phone booth because the police intruded upon his REOP. As a result, the REOP test expanded the Fourth Amendment’s reach and provided Katz with protection against the government’s seizure of the contents of his conversation.

Despite the promise of *Katz*, the REOP test has not been applied expansively in subsequent cases, and the Court has held that many activities that occur in public are not protected against government surveillance. For example, in *United States v. Knotts*, the Court held that the police may monitor a beeper (placed in a bottle of chloroform) to determine where Knotts was traveling. Knotts argued that police use of the beeper constituted a “search” because the police obtained information from the beeper—in particular, the location of a remote cabin where Knotts was manufacturing drugs—that they could not have easily obtained otherwise. Had they tried to follow Knotts, he may have noticed them and either tried to elude them or not gone to the cabin. However, the Court construed the situation very narrowly, concluding that an individual has a diminished expectation of privacy in an automobile, especially when he is traveling on a public highway, and concluded that the beeper simply allowed the police to monitor things that they could have observed from the highway with their own eyes. In other words, had the police been on the road, they could have seen Knotts drive from the city to his remote cabin. Although Knotts had an EOP in

62. *Id.* at 277.
63. *See id.* at 281 (“‘One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one’s residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.’” (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion))). The *Knotts* Court explained:

A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen [a codefendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

*Id.* at 281–82.
64. *Id.* at 285. The *Knotts* Court went on:

A police car following Petschen at a distance throughout his journey could have
the interior of his cabin (which was not infringed), he could not claim a REOP for his drive to the cabin: “A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”

Likewise, in Florida v. Riley, even though the Court had previously placed great emphasis on protecting the curtilage surrounding a home and a homeowner’s EOP associated with the curtilage, the Court held that there was no search when the police flew a helicopter at low altitude over the defendant’s property, thereby allowing them to peer down onto the property. From the fly-over, the police were able to see that the defendant, Riley, was growing marijuana inside a greenhouse. In the Court’s view, Riley had no expectation of privacy because “[a]ny member of the public could legally have been flying over Riley’s property in a helicopter at the altitude of 400 feet and could have observed Riley’s greenhouse. The police officer did no more.”

In California v. Greenwood, the Court upheld a police search of a defendant’s garbage. The Court emphasized that, while the trash was lying by the curb, it was accessible to “animals, children, scavengers, snoopers, and other members of the public,” and the trash had been placed by the curb “for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents’ trash or permitted others, such as the police, to do so.” As a result, since the Greenwoods left their trash by the curb, “in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,” the Court concluded

---

observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car. This fact, along with others, was used by the government in obtaining a search warrant which led to the discovery of the clandestine drug laboratory. But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.

Id. at 281. The Court added that “no such expectation of privacy extended to the visual observation of Petschen’s automobile arriving on his premises after leaving a public highway, nor to movements of objects such as the drum of chloroform outside the cabin in the ‘open fields.’”

Id. at 282 (quoting Hester v. United States, 265 U.S. 57, 59 (1924)).

65. Id. at 281.
67. Id. at 448.
68. Id. at 451.
70. Id. at 40.
71. Id. at 40–41 (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981)) (internal quotations omitted).
that the Greenwoods could not have maintained a “reasonable expectation of privacy in the inculpatory items that they discarded.”

In general, the Court has only reined in governmental surveillance when the government has infringed on someone’s home or private space. For example, in United States v. Karo, a case that is similar to Knotts in that the police used a beeper to track the defendant’s movement to a remote location, the Court held that the use of a tracking beeper violated a homeowner’s REOP because police continued to monitor the location of the beeper even after it was taken inside a dwelling and were thereby able to know when the bottle containing the beeper was moved to another location. The Court reasoned that a search occurs when the government

[S]urreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house. The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched.

Thus, the beeper revealed “a critical fact about the interior of the premises” that the government “could not have obtained without a warrant.” By contrast, the beeper in Knotts “told the authorities nothing about the interior of Knotts’ cabin.” The information obtained in Knotts was “voluntarily conveyed to anyone who wanted to look,” whereas in Karo, “the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified.”

Likewise, in Kyllo v. United States, the Court concluded that the police conducted a search when they pointed an Agema Thermovision 210 thermal imager (essentially, a forward-looking infrared detection device) to scan Kyllo’s home to detect and measure the heat that was being emitted. They did so because they believed (correctly, as it turns out) that Kyllo was growing marijuana in his attic using special lighting

---

72. Id. at 41.
73. See United States v. Karo, 468 U.S. 705, 714 (1984) (“This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. Contrary to the submission of the United States, we think that it does.”).
74. Id. at 715.
75. Id.
76. Id.; see United States v. Knotts, 460 U.S. 276, 285 (1983) (“[T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.”).
77. Karo, 468 U.S. at 715 (quoting Knotts, 460 U.S. at 281) (internal quotations omitted).
78. Id.
(which gave off heat to simulate the effects of the sun) to help the plants grow. 80 Even though the heat might have been observed from the street (for example, by watching how quickly snow melted on Kyllo’s house versus the surrounding houses, or by watching how quickly rain dried), the Court held that police use of the device constituted a search within the meaning of the Fourth Amendment because it could have revealed intimate details regarding the interior of the home (for instance, the time at which the lady of the house takes her bath). 81

Perhaps the only real restraint on the use of surveillance technologies in public spaces was rendered in the case of Carpenter v. United States. 82 In Carpenter, the police used cell site sector information to ascertain a suspect’s whereabouts at the time that certain robberies were committed. 83 Through the use of that data, they were able to ascertain that Carpenter was in close proximity to the robbery sites at the time of the robberies. 84 Thus, the police were able to pinpoint Carpenter’s public movements using technology. One could argue that there was no search in this case. After all, the cell site data revealed nothing more than Carpenter’s location, and the police were particularly interested in knowing about Carpenter’s movements in public (similar to what they were seeking in Knotts). 85 Moreover, although the Court had previously suggested that information that individuals share with others (as they do when their cell phones reveal their locations to cell site towers) does not come with an EOP, the Court nonetheless held that Carpenter held a REOP in his cell site data. 86 The Court noted “society’s expectation... that law enforcement agents and others would not—and indeed could not—secretly monitor and catalogue every movement of an individual’s car for a very long period.” 87 The Court concluded:

Mapping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts... The time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his “familial, political, professional, religious, and sexual associations.” 88

The difficulty is that the Court’s existing precedent imposes few other limits on the ability of the government to observe what happens in public

80. Id. at 29–30.
81. Id. at 34–35, 38–39.
83. Id. at 2212.
84. Id. at 2213.
86. Carpenter, 138 S. Ct. at 2217.
87. Id.
88. Id. (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).
places, to capture that information with CCTV or drones, or to use FRT to help police analyze the images that they have captured. On the contrary, the Court has made it clear that there is a very low EOP for activities that take place in public. Several of the decisions discussed above illustrate that principle. *Riley* suggests that the government can fly over private property and peer down into the curtilage surrounding a home, and *Knotts* suggests that the government can monitor activities that take place in private places.\(^{89}\) Thus, CCTV and drone monitoring of public places may be permissible. Moreover, the U.S. Supreme Court has not rendered any decisions regarding governmental use of FRT, so there is no indication that this technology will be prohibited. *Carpenter* is the only decision that suggests any limits on the government’s ability to monitor what happens in public places.\(^{90}\) However, in that case, the Court did nothing more than limit the government’s ability to access historical cell site data.\(^{91}\)

**CONCLUSION**

Modern technologies have enhanced the ability of governments to spy on the citizenry. Although there has been significant controversy regarding the use of surveillance technologies in countries like China, the problem exists in most Western countries as well.\(^{92}\) In the United States, the government is increasingly using technologies like drones, CCTV, and FRT to spy on people. While these surveillance technologies can serve many important and benign governmental purposes (for example, to locate lost hikers or help ascertain the level of damage in a disaster), as well as to apprehend criminal perpetrators, there is a fear that new technologies can create an Orwellian level of surveillance for everything that occurs outside the home.

Some state and local governments have placed significant limitations on the ability of private individuals and companies to use surveillance devices. For example, Illinois’ Biometric Information Privacy Act (BIPA), sets forth various notice requirements for private entities that collect “biometric identifiers” and “biometric information.”\(^{93}\) BIPA also places restrictions on the ability of private employers to collect biometric

---

90. Compare Carpenter, 138 S. Ct. at 2220–21 (holding that the warrantless access of a person’s cell phone location history violated the Fourth Amendment), with Knotts, 460 U.S. at 281–85 (holding that the use of a radio transmitter in a suspect’s car was not a search or seizure under the Fourth Amendment), and Riley, 488 U.S. at 451–52 (holding that police do not need a warrant to observe a home’s curtilage from navigable airspace).
91. Carpenter, 138 S. Ct. at 2223.
93. 740 ILL. COMP. STAT. § 14/15(b) (2008).
information regarding their employees. Likewise, the California Consumer Privacy Act (CCPA), places limitations on the ability of businesses to collect information, including biometric data. But even in the private arena, the protections are far from comprehensive. For example, the Brookings Institution estimates that private actors will soon have as many drones as the government. One potential restriction is that some companies have indicated that they will limit their sale, research, and development of FRT.

If governmental use of technology like CCTV, drones, and FRT is going to be controlled and limited, Congress will have to exert control through legislation. It is unlikely that courts will do so through their decisions. The U.S. Supreme Court’s search-related jurisprudence has evolved very slowly. In its early decisions regarding technology, the Court was relatively unwilling to rein in governmental use of advanced technologies. Katz was the first decision to explicitly acknowledge and attempt to deal with that problem, and it took the Court nearly half-a-century to get to that point. However, as noted, the Katz test has proven difficult to apply and has not provided consistent or reliable protections to the citizenry. In more recent decisions, such as Karo, Kyllo, and Carpenter, the Court has expanded Fourth Amendment protections on a piecemeal basis, and perhaps the Court will expand its jurisprudence even further in an effort to deal with the implications of technologies like CCTV, FRT, and drones. But the Court has struggled with the problem of advancing technology for nearly a century, and jurisprudential changes have come slowly and haltingly.

It seems unlikely that Congress will deal with the problem either. Congress has been stuck in gridlock for years, and it matters not which party is in power. So, change may have to come at the state and local levels, but those changes will vary by state and will inevitably be piecemeal. Just as some jurisdictions have sought to limit the use of FRT in police investigations, they have the power to impose limitations on governmental use of drones and CCTV. Of course, there is a push-pull

94. Id. § 14/15(b)(3).
98. See Weaver, supra note 1, at 1137 (“[E]arly United States Supreme Court decisions dealing with technology and the Fourth Amendment tended to adhere to more traditional views of the Fourth Amendment and were virtually unresponsive (except in the dissents) to the problems presented by new technologies.”).
here. The public has a strong interest in controlling crime and in protecting itself against criminals, and drones, FRT, and CCTV help the police achieve that objective. The trick for state and local governments is to find an acceptable balance between crime control and privacy protections. Undoubtedly, these are issues that society will debate for many years to come.