Public Governance, Administration and Finances Law Review Vol. 6. No. 2. (2021) • 53–65.

DOI: 10.53116/pgaflr.2021.2.5

The Constitutional Implications of Drones, Facial Recognition Technology and CCTV

Russell Weaver*

* Professor of Law and Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law, e-mail: russ.weaver@louisville.edu

Abstract: Over the centuries, new forms of surveillance technology have emerged. At the founding of the U.S., the government did not have sophisticated spying and surveillance technologies at its disposal. In the eighteenth century, the police might have tried to eavesdrop on their fellow citizens in taverns or other public settings, or they might have listened outside a suspect's window. However, without the advanced technologies that exist today, the opportunities for successful eavesdropping were very limited. Today, surveillance technologies have gone high tech, creating Orwellian possibilities for snooping. As one commentator observed as far back as 1974, "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". This article examines how the U.S. courts are dealing with three different types of technology: CCTV, facial recognition and drones.

Keywords: search and seizure, technology, surveillance, police investigations

Throughout history, advances in technology have profoundly influenced various areas of the law (Weaver, 2019). In the free speech area, for example, Johannes Gutenberg's development of the printing press revolutionised communication and led to revolutionary changes in government (Weaver, 2019, pp. 14–18), religion (Weaver, 2019, pp. 13–14) and science (Weaver, 2019, p. 13). Over time, as new technologies were developed (e.g. the telegraph, the radio, the television, cable and satellite communications and the Internet), people were able to communicate on a scale never seen before (Weaver, 2019, pp. 39–46, 61–65). With the development of the Internet, ordinary people were able to communicate their ideas widely (Weaver, 2019, pp. 39–46, 67–114), largely free (except on social media networks) from the traditional "gatekeepers" who had controlled the use of prior technologies. In the process, governments were toppled and societies were altered (Weaver, 2019, pp. 21–38, 47–60).

In the privacy arena, the changes have been equally profound (Weaver, 2011). At the founding of the United States of America (U.S.), the Government did not have sophisticated spying and surveillance technologies at its disposal. In the eighteenth century, the police might have tried to eavesdrop on their fellow citizens in taverns or other public settings, or they might have listened outside a suspect's window. However,

without the advanced technologies that exist today, the opportunities for successful eavesdropping were very limited. The situation is far different today. Surveillance technologies have gone high tech, creating Orwellian possibilities for snooping (Orwell, 1949). As one commentator observed as far back as 1974, "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" (Amsterdam, 1974, p. 385).

Electricity was the transformative invention for both communications and surveillance. In the communications arena, electricity led to new technologies which made it possible for information to move much more quickly than people could move, and permitted the transmission of both audio and video images over long distances very quickly (Weaver, 2019, pp. 39–46). Regarding privacy, electricity profoundly affected the privacy of individuals as super-sensitive microphones were developed that allowed people to overhear conversations from far away,[1] as well as through walls,[2] and facial recognition and closed circuit television systems allowed governments to maintain continuous surveillance of public places (Temple-Raston & Smith, 2007). Global Positioning System monitoring systems allowed the police to monitor the location and movements of individuals and things,[3] and X-ray technology enabled the police to peer through walls and into the privacy of homes using drive-by X-ray vans (Greenberg, 2010; Basha, 2003). As personal computers and the internet were developed, devices were created which allowed people to monitor the key strokes and computer uses of others,[4] and to do so from distant places using spyware technology (Blakley, Garrie & Armstrong, 2005; Broberg, 2001; Foley, 2007). Moreover, many of these devices were freely available to the public which can purchase devices that allow them to spy on the movement of others,[5] and monitor what their neighbours or others are saying,[6] even from some distance away.[7]

This article focuses on one context in which the new technologies are used: Governmental monitoring of citizens in public places with such technologies as drones, facial recognition technology (FRT) and closed-circuit television (CCTV). As will be seen, in the U.S., there are few restrictions on governmental use of these technologies.

---

1 See *Silverman v. United States,* 365 U.S. 505 (1961) (discussing the fact that advanced surveillance technologies were already available in the 1960s); see also *Katz v. United States,* 389 U.S. 347 (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).

2 See *Goldman v. United States,* 316 U.S. 129 (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).

3 See *City of Ontario v. Quon,* 130 S. Ct. 2610 (2010); *Devega v. State,* 286 Ga. 448, 689 S.E.2d 293 (2010).

4 See the computer spyware devices sold by the USA Spy Shop at www.usaspyshop.com/spy-software-c-55.html

5 See the GPS systems sold by USA Spy Shop at www.usaspyshop.com/gps-tracking-devices-c-118.html

6 See the Spy Zone at www.spyzone.com/ccp0-display/listeningdevices.html

7 See the listening device sold by USA Spy Shop at www.usaspyshop.com/sound-amplifier-system-p-472.html

7. The development of newer technologies

Increasingly, drones, FRT and CCTV are being used by governments to monitor what happens in public spaces.

7.1. Drones

In recent decades, governmental entities have made extensive use of drones (essentially, very small flying machines which are remotely operated by "pilots" who are not on board) for surveillance purposes. Indeed, by 2018, some 910 state and local public safety agencies had purchased drones, including 599 law enforcement agencies. Drones can be equipped with high-powered cameras (e.g. the DJI Zenmuse Z30) that allow them to magnify images on the ground by 180 times, thereby making them effective spies who can create detailed pictures of what is happening below. As a result, drones can observe activities that may not be observable from ground level, including things that are happening in individuals' backyards (Laperruque & Janovsky, 2018).

7.2. Facial recognition technology

Facial recognition technology uses biometric software to map a person's facial features from a video or photo. The technology can then be used to identify the person by pinpoint matching his/her facial features with information contained in existing databases (Collins, 2019).

7.3. CCTV

Closed-circuit television is increasingly being used to monitor what goes on in public places.[8] For example, in the London Underground, there is a pervasive CCTV system which includes some 15,516 cameras.[9] The U.S. is 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 (Plautz, 2019).

[8] See EPIC Surveillance Oversight Project at https://epic.org/privacy/surveillance
[9] See https://bit.ly/3FuO0i5

8. The benefits of drones, FRT and CCTV

Unquestionably, drones, CCTV and FRT offer enormous benefits to governmental officials in their efforts to serve the public. For example, when hikers are lost in remote areas, drones can be used to help locate them (Higgins, 2020). Likewise, following hurricanes, drones can be used "to assess damage, locate victims, and deliver aid". In an effort to prevent forest fires, drones can survey forests equipped with thermal imaging cameras. Drones can also be used to monitor the health and well-being of wild animals (CB Insights, 2020).

Closed-circuit television and FRT have also been enormously helpful in locating and apprehending criminal suspects (Collins, 2019). Closed-circuit television can provide continuous monitoring of public areas, including a photographic record, so that the police can review tape and identify suspects after a crime has been committed (IFSEC Global, 2021). Following the London subway bombings in July 2005, during which 52 people were killed and another 700 were injured (CNN, 2020), the bombers were identified through police review of London Underground CCTV footage (BBC, 2010). Similarly, the Boston Marathon bombers, who killed three people and injured hundreds of others, were found and apprehended using CCTV images captured on government and private cameras. The bombers stood out on the video because of the way they acted: While the crowd was fleeing the scene, the Tsarnaevs lingered around or walked away casually (Kelly, 2013). In tracking down those who attacked the U.S. Capitol Building on 6 January 2021, the Federal Bureau of Investigation (FBI) used CCTV images and FRT, among other techniques (Harwell & Timberg, 2021).

9. Privacy concerns

As facial recognition technology, 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" (Harwell & Timberg, 2021). The use of modern technologies raises Orwellian concerns, and many are uncomfortable with the idea of allowing governments to fly drones over cities, constantly surveilling the actions of citizens. For example, when New York City announced that it was going to deploy some 14 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" (Romero, 2018). 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 building a permanent archive of drone footage of political activity and intimate private behavior visible only from the sky."[10]

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

[10] See BBC (2010) quoting New York Civil Liberties Union associate legal director Christopher Dunn.

map out a biometric profile that is as individually 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" (Sullivan, 2013). One report denounced FRT as "an unreliable, biased and dystopian threat to privacy" (O'Brien, 2020) As the American Civil Liberties Union stated in a report: "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" (American Civil Liberties Union, 2021). Nevertheless, FRT use seems to be expanding and is now used by U.S. Customs and Border Patrol.[11]

Closed-circuit television raises similar concerns. As one commentator argued: "The 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."[12] Closed-circuit television is particularly potent when it is combined with FRT: It accumulates a mountain of facial images that can then be fed into an FRT system to identify people.

The difficulty is that current FRT and CCTV technology provide only a glimpse of what is to come. The FBI is spending more than a billion dollars on expanding its Next Generation Identification (NGI) system.[13] That system will include huge amounts of information about people, including iris scans, photos, palm prints, gait and voice recordings, scars, tattoos and DNA.[14]

10. Legal limitations

There are few meaningful limits on governmental use of 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. For example, the Electronic Privacy Information Center notes that several U.S. cities (e.g. San Francisco, California, Somerville, Massachusetts and Oakland, California) have banned the use of FRT,[15] and the State of California has imposed a moratorium on its use.[16] There are few restrictions on governmental use of CCTV as well.

[11] See https://epic.org/state-policy/facialrecognition

[12] See Slobogin (2002), p. 213, 215.

[13] See www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

[14] The Electronic Privacy Information Center's "Next Generation Identification – FBI" article notes that, in the U.S., there are some restrictions on the use of facial recognition technologies. For example, Boston, Portland and San Francisco have banned the use of facial recognition technologies. In addition, "IBM made the surprising announcement that it would stop selling, researching, or developing facial-recognition services. Amazon and Microsoft followed with their own announcements that they would not sell facial-recognition services or products to state and local police departments, pending federal regulation".

[15] See https://epic.org/state-policy/facialrecognition

[16] Ibid.

There are some restrictions on the government's use of drones. For example, many states have extensive provisions governing the flying of drones by private citizens, but these laws place few restrictions on governmental use.[17] The federal government does impose some limitations on drone pilots. For example, governmental "pilots" must either comply with Federal Aviation Administration Rule 107 waiver requirements,[18] or obtain a federal Certificate of Authorization.[19] In addition, drones cannot be flown within 400 feet of the ground, and may not fly over such venues as military bases or public landmarks.[20]

One would hope 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".[21] Historically, the Fourth Amendment prohibited only "trespassory" invasions against individuals or into "constitutionally protected areas".[22] That approach provided few protections against the use of advanced technologies in public places (Weaver, 2011). For example, in *Olmstead v. United States,*[23] 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".[24] In other words, the wiretapping was permissible because it was done from a public place. Likewise, in *Goldman v. United States,*[25] when the police placed 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.[26]

It took many decades before the Court began to come to grips with the reality of advancing technologies. The Court's landmark decision in *Katz v. United States,*[27] involved a man who the police suspected was involved in illegal bookmaking

---

[17] For a comprehensive list of state drone laws see https://uavcoach.com/drone-laws

[18] See www.faa.gov/uas/commercial_operators/part_107_waivers

[19] See www.faa.gov/uas/commercial_operators

[20] See www.faa.gov/uas/critical_infrastructure

[21] U.S. Const., Amdt. IV.

[22] See, e.g., *Goldman v. United States,* 316 U.S. 129 (1942); *Olmstead v. United States,* 277 U.S. 438 (1928); *Ex Parte Jackson,* 96 U.S. 727 (1877).

[23] 277 U.S. 438 (1928).

[24] Ibid. 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."

[25] 316 U.S. 129 (1942).

[26] Ibid. 135: "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."

[27] 389 U.S. 347 (1967).

operations. Police, anticipating that Katz would make a call from a particular phone booth, placed an electronic bug on the outside of the booth which enabled them to record Katz's incriminating statements, and 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[28] since there was no "intrusion" into the phone booth, and there was doubt about whether the booth would qualify as a "constitutionally protected area". Certainly, under the Court's precedent, there was merit to the government's argument. 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",[29] and held that a search occurs when governmental officials violate Katz's "expectation of privacy".[30] In doing so, the Court purported to shift the focus under the Fourth Amendment from places to persons.[31] As the Court 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."[32] Justice Harlan, concurring, agreed with the Court that the focus should be on whether Katz had an expectation of privacy, but he argued that the expectation must be one that society was prepared to recognize as "reasonable".[33] Ultimately, Harlan's requirement of "reasonableness" was integrated into the EOP test so that the Court inquired whether the police had intruded upon an individual's "reasonable expectation of privacy".

Thus, after *Katz,* the Court used two tests to determine whether a "search" occurred under the Fourth Amendment. In addition to the reasonable expectation of privacy 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,*[34] 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

[28] Ibid. 352.

[29] Ibid. 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."

[30] Ibid. 351–352.

[31] Ibid. 351. "For the Fourth Amendment protects people, not places."

[32] Ibid. 351.

[33] Ibid. 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'."

[34] 565 U.S. 400 (2012).

invalidated the warrantless attachment of the device – and its use to monitor the defendant's car on public streets.[35]

Unfortunately, in the decades since the *Katz* test was announced in the 1960s, it has not provided a workable or reliable test for evaluating Fourth Amendment claims (Weaver, 2011). The reasonable expectation of privacy test could have led to a significant expansion of the Fourth Amendment's scope of protection. That was true in *Katz*. In that case, under the trespass test, there would have been no search. Under *Katz,* 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 reasonable expectation of privacy. As a result, in that case, the reasonable expectation of privacy 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 reasonable expectation of privacy test was not applied expansively in subsequent cases, and the Court has held that many activities that occur in public are not protected against governmental surveillance. For example, in *United States v. Knotts,*[36] the Court held that the police may monitor a beeper (placed in a bottle of chloroform) in an effort to determine where Knotts was traveling. Knotts had 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 would probably 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,[37] especially when he is traveling on a public highway, and finding that the beeper simply allowed the police to monitor things that they could have observed from the highway with their own eyes.[38] 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 expectation of privacy in the interior of his cabin (which was

[35] Ibid. 406–407: "For 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 [or] 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" *United States v. Knotts,* 460 U.S. 276, 286 (1983) (Brennan, J., concurring). 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. We do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."

[36] 460 U.S. 276 (1983).

[37] Ibid. 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" *Cardwell v. Lewis,* 417 U.S. 583, 590 (1974) (plurality)."

[38] Ibid. 281–282. "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 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."

not infringed),[39] he could not claim a reasonable expectation of privacy 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."[40]

Likewise, in *Florida v. Riley,*[41] even though the Court had previously placed great emphasis on protecting the curtilage surrounding a home, and a homeowner's expectations of privacy 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 it to peer down into the property. From the fly-over, the police were able to observe that Oliver was growing marijuana inside a greenhouse. In the Court's view, Riley had no expectation of privacy because "any 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 officer did no more".[42]

In *California v. Greenwood,*[43] the Court upheld a police search of a defendant's garbage. The Court emphasised that, while the trash was lying by the curb, it was accessible to "animals, children, scavengers, snoops and other members of the public",[44] 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".[45] As a result, since the Greenwoods left the 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 that the Greenwoods could not have maintained a "reasonable expectation of privacy in the inculpatory items that they discarded".[46]

The Court has only reined in governmental surveillance when the government has invaded someone's home or private space. For example, in *United States v. Karo,*[47] a case that was 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 reasonable expectation of privacy 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 "surreptitiously employs

[39] Ibid. 285. "A police car following Petschen at a distance throughout his journey could have 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."

[40] Ibid. 282. "But 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" *Hester v. United States,* 265 U.S. 57 (1924).

[41] 488 U.S. 445 (1989).

[42] Ibid. 452.

[43] 486 U.S. 35 (1988).

[44] Ibid. 40.

[45] Ibid.

[46] Ibid. 40–41.

[47] 468 U.S. 705 (1984).

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 reveals "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"[48]

Likewise, in *Kyllo v. United States,*[49] 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 in order 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 (which gave off heat to simulate the effects of the sun) to help the plants grow. Even though the heat could have been observed from the street (e.g. 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.[50]

Perhaps the only real restraint on the use of surveillance technologies in public spaces was rendered in the case of *Carpenter v. United States.*[51] In *Carpenter,* the police used cell site sector information to ascertain a suspect's whereabouts at the time that certain robberies were committed. 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. Thus, the police were able to pinpoint Carpenter's public movements using technology. 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 expectation of privacy, the Court nonetheless held that Carpenter held a reasonable expectation of privacy in his cell site data.[52] 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". 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. As with GPS information, 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.'"[53]

[48] Ibid. 715.
[49] 533 U.S. 27 (2001).
[50] Ibid. 38–39.
[51] 138 S.Ct. 2206 (2018).
[52] Ibid. 2216.
[53] Ibid. 2217.

The difficulty is that the Court's existing precedent imposes few limits on the ability of the government to observe what happens in public places. On the contrary, the Court has made it clear that there is little expectation of privacy for activities that take place in public. Several of the decisions discussed above illustrate these principles. *Florida v. 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. Thus, CCTV 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. However, in that case, the Court did nothing more than limit the government's ability to access historical cell site data.

11. Conclusion

Modern technologies have enhanced the ability of governments to spy on their citizens. Although there has been much controversy regarding the use of these surveillance technologies in countries like China (Human Rights Watch s. a.), the problem exists in most Western countries as well. In the U.S., the government is increasingly using technologies like drones, CCTV and FRT to spy on people. While these technologies can serve many important and benign governmental purposes (e.g. to locate lost hikers, to help ascertain the level of damage in a disaster or emergency), as well to apprehend criminal perpetrators, there is a fear that new technologies create Orwellian surveillance possibilities for activities that occur 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 sets forth various notice requirements for private entities that collect "biometric identifiers" and "biometric information". The Act also places restrictions on the ability of private employers to collect biometric information regarding their employees.[54] Likewise, the California Consumer Privacy Act places limitations on the ability of businesses to collect information, including biometric data.[55] 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 (Bennett, 2014). One potential restriction is that some companies have indicated that they will limit their sale, research and development of facial recognition technology (Peters, 2020).

If governmental use of technology like CCTV, drones and FRT are going to be controlled, limitations will have to come through legislation. They are unlikely to be mandated by the courts. The Court's search jurisprudence has evolved very slowly. In its

[54] See www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
[55] See https://oag.ca.gov/privacy/ccpa

early decisions regarding technology, the Court was relatively unwilling to rein in governmental use of advanced technologies (Weaver, 2011). *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 *Riley,* 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 been struggling with the problem of advancing technology for nearly a century, and jurisprudential changes have been slow and halting.

Of course, the difficulty is that Congress has been stuck in gridlock for decades, and it matters not which party is in power. So, change may have to be driven at the state and local levels, but those changes are likely to vary by state and potentially to 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 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. Thus, 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 in the coming years and hopefully bring to a satisfactory resolution.

References

American Civil Liberties Union (2021). 2019 Proved We Can Stop Face Recognition Surveillance. Online: https://bit.ly/3oHLNJB

Amsterdam, A. G. (1974). Perspectives on the Fourth Amendment. Minnesota Law Review, 58, 349–477.

Basha, R. M. (2003). *Kyllo v. United States:* The Fourth Amendment triumphs over technology. Brandeis L. J., 41, 939.

BBC (2010, October 13). 7 July bombers spotted on CCTV after exhaustive hunt. Online: www.bbc.com/news/uk-11534951

Bennett, W. C. (2014). Civilian drones, privacy, and the federal-state balance. The Brookings Institution. Online: https://brook.gs/3cv40UM

Blakley, A. F., Garrie, D. B., & Armstrong, M. J. (2005). Coddling spies: Why the law doesn't adequately address computer spyware. Duke Law & Technology Review, 25(1).

Broberg, J. (2001). From CALEA to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretape Digital Telecommunications. North Dakota Law Review, 77(4), 795–825.

CB Insights (2020, January 9). 38 ways drones will impact society: From fighting war to forecasting weather, UAVs change everything. Online: https://bit.ly/3kTEDR8

CNN (2020, June 18). 7 July 2005 London Bombings Fast Facts. Online: https://cnn.it/3qQOI5f

Collins, T. (2019, December 23). Facial recognition: Do you really control how your face is being used? USA Today.

Electronic Privacy Information Center (s. a.). Next Generation Identification – FBI. Online: https://epic.org/privacy/fbi/ngi.html

Foley, J. (2007). Are Google searches private? An originalist interpretation of the Fourth Amendment in online communication cases. Berkeley Technology Law Journal, 22(1), 447–475.
Greenberg, A. (2010, September 9). Scanner vans allow drive-by snooping. Forbes. Online: https://bit.ly/3cvMlMV
Harwell, D., & Timberg, C. (2021, April 2). How America's surveillance networks helped the FBI catch the Capitol mob. The Washington Post. Online: https://wapo.st/3qRN57j
Higgins, H. (2020, January 20). Search and rescue teams use drone to help injured hiker in Southern Utah. Fox 13. Online: https://bit.ly/3cpiq98
Human Rights Watch (s. a.). Mass Surveillance in China. Online: https://bit.ly/3DywxVw
IFSEC Global (2021). Role of CCTV Cameras: Public, Privacy and Protection. Online: https://bit.ly/3kQ5VYN
Kelly, H. (2013, April 26). After Boston: The pros and cons of surveillance cameras. CNN Business. Online: https://cnn.it/2Z0xff4
Laperruque, J., & Janovsky, D. (2018, September 25). These police drones are watching you. Project on Government Oversight. Online: https://bit.ly/30EaWw8
O'Brien, S. (2020, March 9). Time to face up to Big Brother. New Haven Independent. Online: https://bit.ly/3qQBe9C
Orwell, G. (1949). Nineteen Eighty-Four. Secker & Warburg.
Peters, J. (2020, June 8). IBM will no longer offer, develop, or research facial recognition technology. The Verge. Online: https://bit.ly/3x13Q0S
Plautz, J. (2019, September 23). Six US cities top list of world's most surveilled. Smart Cities Dive. Online: https://bit.ly/3x4zo5X
Romero, D. (2018, December 4). NYPD to deploy drone fleet, stoking fears of Big Brother. U.S. News. Online: https://nbcnews.to/3Hy3gN4
Slobogin, Ch. (2002). Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity. Mississippi Law Journal, 72, 213–299. Online: https://doi.org/10.2139/ssrn.364600
Sullivan, G. P. (2013, July 9). Big Brother's tracking shines light on emerging facial recognition technology. Forbes. Online: https://bit.ly/3oIp7sx
Temple-Raston, D., & Smith, R. (2007, July 8). U.S. Eyes U.K.'s Surveillance Cameras. National Public Radio. Online: https://n.pr/3cufOqo
Weaver, R. L. (2019). From Gutenberg to the Internet: Free Speech, Advancing Technology and the Implications for Democracy. 2nd ed. Carolina Academic Press.
Weaver, R. L. (2011). The James Otis Lecture: The Fourth Amendment, Privacy and Advancing Technology. Mississippi Law Journal, 80, 1131–1227.