11-28-2016

Advanced Surveillance Technologies: Privacy and Evidentiary Issues

Tina Zheng

Tina Zheng

Professors Daniel Blackaby, Femi Cadmus and Mark Williams

Law Practice Technology

November 28, 2016

Advanced Surveillance Technologies: Privacy and Evidentiary Issues

I. BACKGROUND

Surveillance technology, which encompasses a large array of technologies used to observe individuals' activities and communications, has advanced at a rapid pace and is becoming more widely available in the general marketplace. This trend is potentially caused by increasing fears of terrorism following the September 11 attacks as well the ability of surveillance technology manufacturers to produce the technology at lower costs.[1] Although surveillance technology has long been used by the military and government intelligence agencies, the use of this technology by law enforcement and now private individuals in areas not of national security concern is new and raises privacy and evidentiary issues yet to be settled by U.S. courts.

While it is impossible for traditional surveillance cameras to scan large areas simultaneously over long periods of time, Ohio-based company Persistent Surveillance Systems has created a powerful surveillance device that can track people and vehicles across geographic areas the size of small cities for multiple hours at a time.[2] British company Satellite Applications (SA) Catapult has created the TechDemoSat-1, an advanced satellite "sensitive enough to pick up rabbit holes under bushes," and the number of satellites that it will have launched is scheduled to double in the next decade.[3] Intelligent video analytics allows security software to "learn what is normal" by observing objects in a monitored environment and receiving operator feedback to

incorporate into the system.[4] Intelligent video analytics then analyzes surveillance footage in real-time and detects abnormal activities that humans may overlook, particularly considering the limitations of the human attention span.[5] In short, the government, private businesses, and individuals can now access a host of advanced surveillance technology to identify, locate, and trace individuals, and these technologies have already been used in political demonstrations, traffic impact studies, and security at sporting events.[6]

II. PRACTICAL IMPLICATIONS

Proponents argue that installing these powerful cameras and satellites may deter crime to such an extent that would in turn result in higher property values, improved education systems, increased economic development, and decreased incarceration rates.[7] Key areas of focus for law enforcement would include organized crime, human and drug trafficking, and smuggling.[8] The technology can also be used in more creative manners—for example, Greek officials used satellite imagery to pinpoint houses with undeclared pools, tracking down tax evaders.[9] In the civil litigation realm, advanced surveillance devices can uncover violations of zoning ordinances and environmental regulations.[10] On the global level, this new technology can improve international security, going so far as to assist in the enforcement of arms reduction treaties.[11] From a purely economic standpoint, more advanced technology means more efficiency as scarce government resources are shifted away from law enforcement to other sectors.

However, opponents of the widespread use of advanced surveillance technologies argue that terrorism, the initial reason for the rise of this technology, will not be reduced because terrorists are not deterred by surveillance and may even welcome the publicity that it provides.[12] With regards to domestic crimes, advanced surveillance systems may be more expensive than investigating these crimes after the fact; Britain spends roughly 20 percent of its criminal justice

budget on its video surveillance system.[13] Advanced surveillance technologies also open up the possibility of abuse on a personal level, namely using the technology to blackmail, spy, and harass.[14] Historically, surveillance has focused disproportionately on people of color, which will likely continue to be of concern as the technology advances.[15] Increased surveillance "will have a chilling effect on public life," making law-abiding citizens more self-conscious and less able to enjoy themselves in public spaces.[16] Even assuming that advanced surveillance technologies do in fact serve all of its public policy goals, its use, particularly by private entities, raises fundamental privacy and evidentiary concerns.[17]

III. PRIVACY INFRINGEMENT

Although using satellites to aid in investigations is not new, recent technological advances enable much more accurate and reliable imagery,[18] which can be seen as an infringement of privacy and a move towards an Orwellian, totalitarian society. To contrast, most images in Google Earth's database are taken at an aerial view of 800 to 1,500 feet and updated monthly on a rolling basis.[19] However, for satellites developed in the past few years, pixel resolution has increased from five meters to thirty centimeters, and visual imagery is updated in real-time.[20] And because most of these advanced surveillance technologies are commercially owned, individuals who have the financial resources to purchase them may use them to "spy" on others with great precision.[21]

The Fourth Amendment guarantees citizens the right "to be secure in their persons [and] houses . . . against unreasonable searches and seizures."[22] To determine that there has been a Fourth Amendment violation, an individual must show that (1) "he seeks to preserve something as private"; and (2) his "expectation [of privacy], viewed objectively, is justifiable under the circumstances."[23] As in the case of any cutting-edge technology, case law has been slow to catch

up with advancements in surveillance technology, leaving it unclear what constitutes "unreasonable searches and seizures" under the Fourth Amendment.

To analogize, courts have generally permitted law enforcement to use aerial surveillance so long as the footage "captures images visible to the naked eye."[24] Footage capturing images not visible to the naked eye may constitute an unconstitutional search under the Fourth Amendment when filmed without first obtaining a warrant.[25] Although current surveillance technology is mostly limited to tracking the location of vehicles and individuals, which appear as single pixels[26] likely visible to the naked eye, it is easy to imagine cameras becoming more precise so that the vehicles and individuals may be distinguished from one another and their particular movements monitored, which would not have been otherwise visible to the naked eye. Courts must then decide the issue of whether to prohibit the use of this surveillance technology without a warrant, or to do away with the "naked eye" standard.

Courts do not permit law enforcement to use "advanced technology to observe activities or individuals in areas protected by the Fourth Amendment that would otherwise be unobservable without a physical intrusion into an enclosure, at least where the advanced technology is 'not in general public use.'"[27] But it is unclear to what extent a new piece of technology must spread amongst the general public in order for law enforcement to use it without first obtaining a warrant.[28] Under the "plain view" doctrine, there is no "reasonable expectation of privacy" in that which is knowingly exposed in open view[29] or which is observed by law enforcement from a "lawful vantage point" such as "public navigable airspace" in the case of aerial surveillance.[30] Courts provide little guidance regarding under what circumstances an individual can reasonably expect his or her activities and communications to remain private.

As advanced surveillance devices become more prevalent amongst consumers, the technology considered to be "in general public use" and what constitutes a "reasonable expectation of privacy" will likely expand,[31] thereby giving law enforcement even greater latitude to employ advanced surveillance technologies. There is an underlying concern that advanced technologies will "promote lazy law enforcement," encouraging police officers to take shortcuts when gathering evidence, relying excessively on technology rather than their experience and judgment,[32] further increasing the likelihood of Fourth Amendment infringement. Courts will soon be confronted with the challenge of determining the ability for technology "to shrink the realm of guaranteed privacy."[33]

IV. UNFAIR PREJUDICE AT TRIAL

Even if any given advanced surveillance footage manages to fend off Fourth Amendment attacks, it must still defeat evidentiary concerns in order to be introduced at trial. In criminal trials in the United Kingdom, evidence introduced often comprises of images allegedly of the defendant captured by surveillance cameras, commonly known as closed-circuit television (CCTV), which are ubiquitous in both public and private spaces.[34] Because these graphics can be highly compelling, they may encourage victims and witnesses desperate to nail down the perpetrator to make an identification when there is still reason for doubt.[35] It is easily imaginable that jurors would find advanced surveillance footage even more compelling, increasing the likelihood of placing too much weight on such evidence.

As with any evidence being introduced at trial, the probativeness of advanced surveillance footage must be weighed against its potential for unfair prejudice. Advanced surveillance footage may be seen as highly probative because it is not merely a reenactment or reconstruction; it is recorded contemporaneously and generally considered to be "a fair, accurate,

and authentic representation" of the events that took place.[36] This may seemingly eliminate the need for the party introducing the evidence to lay an extensive foundation for its admissibility.[37] However, jurors' tendency to believe that advanced surveillance footage is always true in turn creates a tendency to believe that the assertions of the party introducing such footage are also true, despite the absence of additional evidence and the presence of reasonable doubt.[38] The level of pull that advanced surveillance footage has on jurors incentivizes the party seeking to admit the evidence to fabricate or alter it, which is possible given that that party likely has complete control over the technology; this phenomenon tilts in favor of establishing a higher standard for admissibility.[39]

Additionally, storage of surveillance footage in searchable databases raises the question of whether in the future an individual may be prosecuted solely on the basis of facial resemblance discovered through a database search.[40] While facial recognition software is currently available to law enforcement, it still relies on human judgment and thus does not meet the "evidential threshold for admission in court."[41] Also, current facial recognition software fails to take into account the fact that a face may change over a short period of time due to an individuals' pose, health, and expression and the fact that some combinations of facial features may be highly prevalent in a population.[42] When these facial recognition issues are combined with surveillance footage taken from various angles and distances, introducing such evidence in court may unfairly prejudice jurors.[43] Defense attorneys confronted with such evidence and required to rebut the inference of the defendant's identity may find themselves unable to do so due to limited resources, knowledge of the technology, and access to satellite interpretation and facial mapping experts.[44]

V. POTENTIAL SOLUTIONS

Because the Supreme Court has yet to decide on Fourth Amendment issues surrounding advanced surveillance technologies, there is no binding precedent for lower courts to apply. However, legislatures can work towards enacting clearly-defined boundaries in the use of advanced surveillance technology—for example, how long data may be stored, when footage may be accessed, and by whom. Police officers should be permitted to access the footage only after a crime has been reported, and only footage surrounding the specific crime should be accessed, thus preventing "fishing expeditions."[45] There must be an enforcement mechanism in place along with a clear set of punishments for violators. Additionally, more invasive advanced surveillance technologies should be reserved for situations in which traditional surveillance technologies are "unavailable, unworkable, or inefficient on a cost or resource basis."[46] Needless to say, all use of advanced surveillance technologies by law enforcement must be approved in advance by government agencies, barring truly exigent circumstances.[47] If advanced surveillance footage was obtained without prior approval or the existence of exigent circumstances, the evidence should be excluded at trial.[48]

If advanced surveillance footage is permitted to be introduced into evidence at trial, jurors should be cognizant of the quality of the evidence and refrain from rendering its decision on the basis of this evidence alone. To aid in this regard, courts should issue jury instructions directing jurors to exercise caution when taking into consideration advanced satellite imaging paired with facial mapping as evidence.[49] Meanwhile, more scientific studies and data gathering can increase the confidence that jurors have in advanced surveillance technologies. As facial recognition software becomes more prevalent, studies of large populations should be conducted to determine the uniqueness of particular facial features and feature combinations to provide a statistical foundation for identification.[50]

[1] ACLU, *What's Wrong with Public Video Surveillance?*, https://www.aclu.org/other/whats-wrong-public-video-surveillance.
[2] Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST (Feb. 5, 2014), https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.
[3] Kieron Monks, *Spy Satellites Fighting Crime from Space*, CNN (Aug. 12, 2014, 5:41 AM), http://www.cnn.com/2014/08/11/tech/innovation/spy-satellites-fighting-crime-from-space/.
[4] Mahesh Saptharishi, *The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology*, WIRED https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/.
[5] *Id.*
[6] *See* Timberg, *supra* note 2.
[7] *See id.*
[8] *See* Monks, *supra* note 3.
[9] Edward Knoedler, *Satellites and Municipalities: One Town's Use of Google Earth for Residential Surveillance*, 28 TOURO L. REV. 421, 426 (2012).
[10] *See* Patrick Korody, *Satellite Surveillance Within U.S. Borders*, 65 OHIO STATE L. JOURNAL 1627, 1629 (2004).
[11] *See* Monks, *supra* note 3.
[12] *See* ACLU, *supra* note 1.
[13] *See id.*
[14] *See id.*
[15] *See id.*
[16] *See id.*
[17] *See* Timberg, *supra* note 2.
[18] Monks, *supra* note 3.
[19] Knoedler, *supra* note 9 at 424.
[20] Monks, *supra* note 3.
[21] *See id.*
[22] Knoedler, *supra* note 9 at 429.
[23] *Id.* at 431.
[24] Timberg, *supra* note 2.
[25] *See id.*
[26] *Id.*
[27] Korody, *supra* note 10 at 1652.
[28] *See* Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 737–38 (2015).
[29] *See id.* at 1645.
[30] *See id.* at 1649.
[31] *See id.* at 1645.
[32] *See* Pearlman & Lee, *supra* note 28 at 728.
[33] *See* Knoedler, *supra* note 9 at 429.

[34] Tony Ward, *Surveillance Cameras, Identification and Expert Evidence*, 9 EVIDENCE & ELEC. SIGNATURE L. REV. 42, 42 (2012).
[35] *See id.* at 43.
[36] *See* 16 AM. JUR. 3D *Proof of Facts* § 1 (1992).
[37] *See id.*
[38] *See* 16 AM. JUR. 3D *Proof of Facts* § 3 (1992).
[39] *See id.*
[40] *See* Ward, *supra* note 34 at 47.
[41] *See id.*
[42] *See id.*
[43] *See id.*
[44] *See id.*
[45] *See* Timberg, *supra* note 2.
[46] *See* Korody, *supra* note 10 at 1660.
[47] *See id.* at 1660–61.
[48] *See id.* at 1661.
[49] *See* Ward, *supra* note 34 at 47.
[50] *See id.* at 43.