International Municipal Lawyers Association
2016 Mid Year Seminar
April 15-18
Washington DC

Public Safety Technologies

Gary W. Schons
Of Counsel
Best Best & Krieger
San Diego, California

©2016 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2016 Mid Year Seminar, held April 15-18, 2016 in Washington, D.C. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Public Safety Technologies

By Gary W. Schons, Of Counsel, Best Best & Krieger
San Diego, California
(619) 525-1348 / gary.schons@bbklaw.com

Introduction

Technological advancements in imaging, positioning, mosaic data collection and mining, bio-metric identification, and activity and sound detection are rapidly being adapted to law enforcement applications, changing and advancing the provision of public safety, security, crime suppression, deterrence, and detection, and the apprehension and prosecution of criminal offenders. In parallel with these developments, the widespread, in fact, nearly universal use of personal, portable electronic devices which communicate in an array of modes and transmit and store troves of data, expose ever more intimate personal details, ranging from precise positions and movements to political and personal expression, to detection, monitoring, interception, analysis and storage. At the crossroads of these applied technologies are concerns for privacy, civil liberties, the expansion and limits of government power, and the shape and contours of ordered liberty in the 21st Century.

The principle constitutional restraint on government (law enforcement) intrusions on "privacy" is the Fourth Amendment prohibition against unreasonable searches and seizures. Since *Katz,*[1] a "search" has been recognized as a "prying into a private place," and a determination of what is "private" has been based on a value-oriented analysis of a person's subjective expectation of privacy which society is willing to recognize as reasonable. Recent technological advances have contorted or bent the notion of "prying" and "privacy" on both ends of the spectrum. For example, armed with technology like infrared detection devices, police can detect heat radiating from a home, indicating ongoing narcotics production. Is this a "prying into a private place," or merely detecting heat emanating from a building? This is a "search."[2] On the other hand , police are generally entitled to search a person's wallet or purse without a warrant incident to an arrest. But, how about a cellphone? Once, but not anymore.[3] Yet, as will be discussed, Fourth Amendment jurisprudence is in a constant race to keep up with advances in police deployed technology and private electronic communication and data storage. In some instances, the judicial footing is halting, and divided. Further, some scholars believe that the Fourth Amendment, alone, cannot protect privacy from and in new technologies.[4]

---

[1] *Katz v. United States*, 389 U.S. 347(1967)
[2] *Kyllo v. United States*, 533 U.S. 27 (2001)
[3] *Riley v. California*, ___U.S. ___, 134 S.Ct. 2473 (2014).
[4] See, Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 *Michigan Law Rev* 801, 838 (2004); Ku, "The Founders' Privacy: The Fourth Amendment and the Power of Surveillance," 86 *Minnesota Law Rev.* 1325 (2002); Cloud, "Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment, " 72 *Miss. Law Journal* 5 (2002).

Two other checks or limits on police "intrusions" on "privacy" through or resulting from the use of advanced technologies can originate in state legislative enactments[5] or arise from media or public scrutiny based on Freedom of Information Act ("FOIA") or Public Records Act ("PRA") disclosures. Legislatures in the states have stepped in on a number of occasions to restrain or limit police searches or data collection and use where the Fourth Amendment or judicial limits do not extend.[6] Media "watchdogs" and civil liberty groups, such as the ACLU, have launched inquiries into law enforcement use of advanced technologies without judicial or "civilian" oversight by obtaining records through FOIA or PRA requests or litigation. Follow-on published exposes have led to public and official scrutiny and changes in practices and procedures.[7] Finally, local police agencies are responding to "civilian" oversite and community concerns over threats to privacy by developing and adopting policies and procedures which guide and restrain law enforcement use of these technologies.[8]

The challenges posed by these advancing technologies for the municipal lawyer in advising and representing law enforcement agencies and their cities are many. First, the municipal lawyer needs to be aware of these technologies, their uses and capabilities and existing legal restraints on their use, whether constitutional or statutory. Second, the municipal lawyer needs to be attuned and sensitive to the public policy implications of the deployment of these technologies, including impacts on privacy, security, public safety and legal liability. Finally the municipal lawyer needs to be a thought-leader in helping to design and implement policy, protocols and best practices for the appropriate and responsible deployment of these technologies.

U.S. Supreme Court Responses at the Crossroads of Law Enforcement and Advanced Technologies

While the United States Supreme Court has grappled with technological advances in law enforcement within the context of the Fourth Amendment prohibition against unreasonable search and seizure for nearly the last one hundred years, the progress of the law has been not been doctrinally consistent. The Supreme Court's 1928 *Olmstead* decision[9], regarding telephone wiretaps, premised the determination of whether a "search" has occurred on the notion of

---

[5] In *United States v. Jones,* ___U.S. ___, 132 S.Ct. 945 (2012), Justice Alito noted in his concurring opinion:"[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping."

[6] For example, in 2015, the California enacted the Electronic Communications Privacy Act to prohibit law enforcement from compelling the production of electronic communication information or electronic device information without a search warrant or court order. (SB 178, adding Section 1546 et seq. to the California Penal Code.)

[7] See, "New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says," *New York Times,* Feb. 11, 2016 http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=0; "Cell-Tracking "Stingray" Device Was Kept Secret," *San Diego Union Tribune,* Feb. 13, 2016, http://www.sandiegouniontribune.com/news/2016/feb/13/cell-tracker-nondisclosure/ ; Cagle (ACLU), "Documents Reveal Anaheim, CA Has Surprisingly Robust Surveillance Arsenal for Small City," Jan. 27, 2016 https://www.aclu.org/blog/free-future/documents-reveal-anaheim-ca-has-surprisingly-robust-surveillance-arsenal-small-city

[8] See, Stanley (ACLU), "Police Body-Mounted-Cameras:With Right Policies in Place, a Win for All," https://www.aclu.org/police-body-mounted-cameras-right-policies-place-win-all

[9] *Olmstead v. United States,* 277 U.S. 438 (1928).

physical trespass, and looked to the place where the search was conducted. The 1967 *Katz* decision largely repudiated the "trespass" doctrine of *Olmstead* and replaced it with a test which focused on whether the search intruded into a place where a person has a subjective expectation of privacy that society was willing to recognize as reasonable.[10] However, over the last decades of the 20th century and early 21st century, the Court drifted back toward giving enhanced preference to certain places, foremost the home,[11] and looked to the nature of the law enforcement intrusion rather than strictly the expectation of privacy, particularly when reviewing the propriety of "sense enhancing" technology employed by law enforcement.

In *Kyllo*, the case previously mentioned involving the use of a thermal imager to detect a marijuana grow operation inside a home, Justice Scalia wrote: "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search---at least where (as here) the technology in question is not in general use."[12] Thus, use of an "exotic" thermal imager might transgress the Fourth Amendment, while use of binoculars would not. Some scholars reacted to this reasoning, in which the Fourth Amendment may not protect people's expectation of privacy once a surveillance or detection device is in general use, as constituting the "Walmart test."[13] Put in another context, surely just a few years ago drones were "exotic" technology. Now they are in the hands of hundreds of thousands of private citizens. Thus, the question arises, because drones are now in general use, can law enforcement make use of drones for surveillance purposes without implicating the Fourth Amendment?[14]

Two fairly recent decisions by the Supreme Court serve to illustrate the challenges facing the bench and bar in applying the Fourth Amendment to new technologies.

United States v. Jones[15] posed the question whether the police attaching a Global-Positioning-System (GPS) tracking device to an individual's vehicle, without benefit of a warrant authorizing that action, and the subsequent use of that device to monitor the vehicle's movements on public streets for 28 days, constitutes a "search" within the meaning of the Fourth Amendment. The government's argument was that under the *Katz* test, Jones had no reasonable expectation of privacy in the exterior of the vehicle where the device was attached and no reasonable expectation of privacy in the locations the vehicle traveled on public roads, which made it visible

---

[10] *Katz v. United States, supra,* 389 U.S. 347.

[11] Compare, *United States v. Knotts,* 460 U.S. 276 (1983) (use of "beeper" to track drug manufacturing products in a vehicle did not require a warrant), with *United States v. Karo* 468 U.S. 705 (1984) (use of an electronic beeper to monitor movement of drug manufacturing products in a home required a warrant), with *Kyllo v. United States, supra*, 533 U.S. 27 (use of thermal imager to detect heat emanating from a residential marijuana grow operation required a warrant).

[12] *Kyllo* at 39.

[13] Christopher Slobgrin, "Peeping Techno-Toms and the Fourth Amendment: Seeing Through *Kyllo's* Rules Governing Technological Surveillance," 86 *Minnesota Law Review* 1393 (2002).

[14] The Supreme Court has twice held that the Fourth Amendment does not require police to obtain a warrant before observing what any other member of the public could with the naked eye, even when that observation takes place in the public airspace. (See, *Florida v. Riley,* 488 U.S. 445 (1989) (police helicopter); *California v. Ciraolo* , 476 U.S. 207 (police in a fixed-winged airplane.) See also, *Dow Chemical Co. v. United States,* 476 U.S. 227 (1986) (EPA's use of a commercial aerial photographer using a precision aerial camera to photograph a chemical plant did not violate the Fourth Amendment).

[15] *United States v. Jones* , *supra*, 132 S.Ct. 945.

to all. The government relied on one of the tenet's of *Katz*, that what a person knowingly exposes to the public, even in his own home or office, is not protected by the Fourth Amendment.[16]

Writing for a unanimous court, Justice Scalia impliedly rejected the government's *Katz* based arguments by averting to the earlier understanding of the Fourth Amendment based on the notion of "trespass" (*Olmstead*).

> "Here, the Court need not address the Government's contention that Jones had no 'reasonable expectation of privacy,' because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' *Kyllo v. United States*, 533 U. S. 27, 34. *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test."

Just as interesting were the concurring opinions. Justice Sotomayor would have found a Fourth Amendment violation based on *Katz's* reasonable expectation of privacy formulation, alone. More significantly, she joined with Justice Alito's concurrence, which was joined by three other justices. Justice Alito criticized and in fact belittled Justice Scalia's trespassory analysis[17], and argued that even without a trespass, which more advanced technology would not require, there would remain a Fourth Amendment violation. Justice Sotomayor wrote:

> "In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But '[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.' [Citation.] As Justice Alito incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. [Citation.] Under that rubric, I agree with JUSTICE ALITO that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' [Citation.]."

What *Jones* seems to predict is that at least a majority of the court would continue to look to *Katz's* reasonable expectation of privacy formulation, which is admittedly elastic, malleable and evolving, in determining whether, in the context of emerging technologies, a Fourth Amendment search has occurred and whether a particular search is reasonable . (A search without a warrant is presumptively unreasonable, subject to certain specifically established and well delineated exceptions; while a search with a warrant is presumptively reasonable.[18].)

---

[16] *Katz* at 351.

[17] In his concurring opinion, Justice Alito poked fun at Justice Scalia's claim that something akin to the GPS monitoring in the *Jones* case could have occurred in 1791 when the Fourth Amendment was considered. "The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience."

[18] See, *Chimel v. California*, 395 U.S. 752, 763 (1969).

For at least forty-five years, the Supreme Court told the police they could without a warrant search the body of a person arrested and the "area into which he might reach" in order to protect material evidence or the officer's safety. This "search incident to arrest" doctrine meant that the police could search the personal effects of a person arrested, such as a purse, wallet, briefcase or backpack. [19]

When San Diego police arrested David Leon Riley for illegal possession of handguns, they searched his person, seized a cellphone found in his pocket, and later searched through the digital information in the phone, including photos, videos and messages, finding evidence connecting Riley to a gang and a gang-related murder. Riley was convicted, in part based on the evidence obtained from his cellphone.

Riley's challenge to this warrantless search eventually found its way to the United States Supreme Court. Riley's counsel argued that his cellphone was not like a wallet, purse, briefcase or backpack, and he warned that it could open up "every American's entire life to the police department, not just at the scene but later at the station house and downloaded into their computer forever."[20]

Writing for a unanimous Court, Chief Justice Roberts concluded that the rationale for the "search incident to arrest" doctrine---to protect material evidence or officer safety---could not justify the wholesale intrusion into the vast trove of a digital data on a cellphone without a warrant.[21] Chief Justice Roberts first dispatched the officer safety concern.

> "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon--say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one."

The Chief Justice then turned the thornier issue of finding and preserving material evidence, which Riley's phone so amply contained. The Chief Justice conceded that cell phone data could be vulnerable to remote wiping, and that an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted. He cited several examples by which the police could either turn off or prevent the phone's security features from activating, thus preserving the data for a later search authorized by a warrant.[22] But, most crucially, Chief Justice Roberts wrote that cell phones differ in both a quantitative and a qualitative sense from other objects in a person's pocket:

---

[19] *Ibid.*

[20] Fuchs, "Supreme Court Hears Case That Could Open Up 'Every American's Life To The Police Department," *Business Insider,* April 29, 2014 http://www.businessinsider.com/supreme-court-hears-riley-v-california-2014-4

[21] *Riley v. California, supra,* 134 S.Ct. 2473.

[22] The Chief Justice could not have anticipated the recent furor and legal proceedings over the FBI's effort to gain access to the San Bernardino terrorist's Apple IPhone, which locked after he was shot and killed and which cannot be opened without Apple creating software to bypass its own security technology. Apple's locking and encryption technology may well have changed this calculus while the ink is barely dry on the *Riley* decision. See, Rosenthal,

> "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."

The *Riley* decision is a stark example of advances in technology, particularly where that technology is in wide spread use, bending the arch of Fourth Amendment analysis. In truth, the search of a wallet, purse or briefcase could be just as intrusive and revealing as searching the digital information in a cellphone.[23] But the storage capacity of the cellphone and the uses to which it has been put in contemporary society, simply overrode the law enforcement considerations which had shaped and sustained the "search incident to arrest" doctrine. This required a re-balancing of law enforcement and privacy interests and resulted in a requirement that police now obtain a warrant before searching the digital data in a cellphone.

What seems to be emerging in the jurisprudence of the Supreme Court and lower federal and state courts,[24] is an examination of scope and nature of the information acquired by the government (police), balanced against the law enforcement interests in acquiring the information ---the tradeoff between the efficiency and efficacy of law enforcement and the privacy rights of citizens in their persons, including movement, communications and identity, residences, and, importantly, personal effects.[25]

Each kind of police applied technology is discussed separately, here. However, it is important for legislative bodies, policy makers, law enforcement executives, and government counsel to be mindful that what concerns citizens, their elected representatives, as well as civil rights and privacy advocates is the synergistic, cumulative and cascading effects of these technologies in combination, powered by massive advancements in computing, data mining and data storage. These effects pit the quest for security against some of our most precious notions of privacy and anonymity and the specter of "Big Brother" looms in these discussions. For example, the ever increasing number of both private and public surveillance cameras, when combined with facial recognition technology, threatens to turn public and private spaces into personal identification bazaars Therefore, inherent in the consideration of the application and implementation of each of these technologies, and the laws and policies governing any one of them, is how the

---

"Why Apple's CEO and the FBI Are Fighting Over Your Phone," *Mother Jones*, Feb. 17, 2016 http://www.motherjones.com/politics/2016/02/apple-ceo-tim-cook-san-bernardino-iphone

[23] Justice Alito noted this anomaly in his concurring opinion, and, as he had in his concurrence in *Jones*, suggested that Congress and the state legislatures may need to consider new laws that draw "reasonable distinctions based on categories of information or perhaps other variables," otherwise "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."

[24] Compare, *United States v. Vargas*, ___F.Supp.2d ___ (E.D. Ore. 2014), (No. CR-13-6025-EFS) (pole mounted camera that surveilled a front yard for six weeks without a warrant violated the Fourth Amendment), with *United States v. Houston*, ___F.3d. ___ (10th Cir. 2016) (14-5800, 2/8/16) (pole mounted camera that surveilled a rural property for 10 weeks did not require a warrant, *Jones* distinguished).

[25] See, e.g., Larkin, "The Fourth Amendment and New Technologies," Heritage Institute Legal Memorandum #102, Sept. 19, 2013 http://www.heritage.org/research/reports/2013/09/the-fourth-amendment-and-new-technologies

deployment of that technology is affected or magnified by other technological developments and advancements.

Stingray

Perhaps the most controversial surveillance technology now in the hands of the police is the Stingray, a cellular telephone surveillance device that operates as an IMSI (or ESN) identifier. An IMSI (or ESN) is a cellphone's unique numeric identifier. Without any action by the phone's owner, cellphones regularly transmit data to cell sites or towers, including the phone's IMSI and the cell site code, which identifies the phone's location with great precision. The IMSI identifier imitates a cell site, collecting this data from all cellphones in the vicinity of the device.

If the police know a suspect's location, it can use the Stingray to determine the unique IMSI of the suspect's cellphone. This information can then be used to obtain call records for the phone or to obtain a wiretap for the phone, itself. Conversely, if the police know the IMSI of the suspect's phone, it can then use the Stingray to determine the phone (and suspect's) location with great precision, at times within seven feet. In certain configurations, the Stingray is capable of capturing the content of communications, such as voice calls and text messages.[26]

The Stingray is compact enough to be carried by hand (trade name KingFish), or can be mounted in a vehicle, a drone or an aircraft. It costs between $350,00 and $400,000.

The concerns over the use of the Stingray device are many. Some of the 48 agencies in 20 states armed with the Stingray device are using the device without a search warrant. [27] The United States Supreme Court has held that pen registers and "trap and trace" devices, which are older technology with functions analogous to those of the Stingray, are not subject to the Fourth Amendment warrant requirement because the user voluntarily conveys the numerical information---numbers dialed and calls received---to the telephone company.[28] However, as noted, a cellphone transmits the IMSI and cell site information without any activity by the user. This may well serve to distinguish this technology from traditional pen registers or "trap and trace" devices for Fourth Amendment purposes.

In November, 2015, Representative Jason Chaffetz (R-Utah) introduced the Cell-Site Simulator Act of 2015, also known as the Stingray Privacy Act, in Congress. The bill would require state and local law enforcement agencies to obtain a warrant before they could use Stingray devices

[26] Federal policy, adopted in October 2015, prohibits such use of the Stingray, effectively a wire intercept. (See, U.S. Dep't of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* (Sept. 2014) http://www.justice.gov/opa/file/767321/download)

[27] With limited exceptions, USDOJ policy requires that federal officers obtain a search warrant based on a showing of probable cause before using the Stingray. (*Ibid*.) California's Electronic Communications Privacy Act (see, note 6, supra) requires officers to obtain a search warrant to use a Stingray device. However, *The New York Times* reported that the NYPD obtains court authorization for use of the Stingray on the lesser standard applicable to pen register devices, namely, that information likely to be obtained from the device is "relevant" to an ongoing criminal investigation. (New York Criminal Procedure Law, Article 705, Section 705.10; see also 18 U.S.C. sec. 206). (http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html .)

[28] *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

under threat of federal criminal prosecution.[29] The bill would also require law enforcement to disclose to a judge or magistrate how the Stingray technology operates, as opposed to some other surveillance tools like pen registers.[30] Five states---California, Minnesota, Utah, Virginia and Washington---have already passed laws requiring its officers to obtain a search warrant before using the Stingray.[31]

Second, although the police may be interested in only the particular cellphone and location of a suspect in a criminal investigation, the device sweeps up all cellphones in the vicinity of the device when it is operating, thus capturing data from "innocent bystanders." There does not appear to be safeguards in place to protect this data. Additionally, law enforcement agencies have been secretive about the devices, citing confidentiality agreements with the manufacturer and the FBI.[32]

A recently enacted law in California addresses both of these concerns. Senate Bill 741 signed into law by Governor Jerry Brown in the fall of 2015 requires local agencies that operate cellular communications interception technology, such as the Stingray device, to maintain operational, administrative, technical, and physical safeguards to protect information gathered through use of the technology from unauthorized access or disclosure. The law, adding section 53166 to the California Government Code, requires local agencies to implement usage and privacy policy, to ensure that the collection, use, maintenance, sharing, and dissemination of information gathered through use of the technology complies with applicable law and is consistent with respect for an individual's privacy and civil liberties. The bill further requires that the local agency make the usage and privacy policy available in writing to the public.[33]

Responsible deployment of the Stingray device is another technological application ripe for careful policy development at the local level to either complement or act as a substitute or placeholder in lieu of judicial and legislative developments.

Cellphone Tower Dumps

A "cellphone tower dump" is an expression for a process when law enforcement seeks information sent from cellphones to a cellphone tower during a given period of time. As

---

[29] "New-Bill-Would-Force-Cops-to-Get-Stingray Warrants," *Wired*, November 3, 2015 http://www.wired.com/2015/11/new-bill-would-force-cops-to-get-warrants-before-spying-with-stingrays/new-bill-would-force-cops-to-get-warrants-before-spying-with-stingrays/

[30] There are documented cases in which police have obtained court orders to authorize trapping cellular telephone information without advising the judge that the Stingray technology would be employed. Wessler (ACLU), "New Evidence Shows Milwaukee Police Hide Stingray Usage from Courts and Defense," Jan. 25, 2016 https://www.aclu.org/blog/free-future/new-evidence-shows-milwaukee-police-hide-stingray-usage-courts-and-defense

[31] California (SB 178 (2015)); Minnesota (SF 2466 (2014)); Utah (1HB128 (2014)); Virginia (HB 1408 (2015); Washington (HB 1440 (2015)).

[32] See, "What is the Big Secret Surrounding Stingray Surveillance?", *Scientific American*, June 25, 2015 http://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/ . Examples have been documented in New York, San Diego, and Anaheim, California referenced in the articles cited in note 7, *supra.*

[33] "Police Slow to Post "Stingray" Policies," *San Diego Union Tribune*, Jan. 13, 2016 http://www.sandiegouniontribune.com/news/2016/jan/13/stingray-policies/

previously noted, cellphone towers enable GPS in cellphones and allow phones to make and receive calls. Cellphones constantly and passively search for a tower to connect to, and relay information even when not in use. That data is saved by the cellphone company for months and years and can include location information, call history, sent texts and even search terms typed into phone browsers.[34]

USDOJ attorneys apply for court orders authorizing "dumps" under the Electronic Communications Privacy Act of 1986.[35] This requires a showing of relevance to an ongoing investigation, but not probable cause as required for issuance of a search warrant. California requires a search warrant,[36] but there is no source accounting for practices in other states. Some scholars have argued that this information is entitled to Fourth Amendment protection which should require a showing of a probable cause and release only pursuant to a search warrant.[37] So far, no U.S. court has adopted this argument, although a Canadian court has.[38] Law enforcement routinely seek thousands of these "dumps" annually.[39]

The concern of civil rights and privacy advocates is that these "dumps" give law enforcement vast amounts of data related to innocent persons, unrelated to any particular investigation. There is no accounting for how this "excess" data is handled.

In Canada, two of the nation's biggest telecommunications companies brought suit in an Ontario court to halt the practice, arguing that sweeping "tower dumps" violate the Charter of Rights and Freedoms.[40] On January 14, the judge ruled there was a breach of the Charter in "tower dump" production orders that required the two telecommunications companies to provide to the police the personal information of about 40,000 users. The judge found that the disclosure of the personal information required went "far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation."[41]

Range-R Radar

Range –R radar is a handheld (10" x 4") Doppler radar device capable of penetrating most common types of building walls, ceilings and floors. While it does not provide an image, it is

---

[34] *USA Today*, "Cellphone Data Spying: It's Not Just the NSA," Dec.8, 2013 http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/

[35] Pub. L. No. 99-509, 100 Stat. 1848 (1986). U.S. Dept. of Justice, Law Enforcement Telephone Investigations Resource Guide 7 (rev. Mar. 10, 2010), available at http://cryptome.org/isp-spy/le-tel-spy.pdf

[36] California Electronic Communications Privacy Act, Cal. Penal Code, secs. 1546 et seq. (SB 178 (2015).

[37] Owsley, "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance," 16 *Journal of Constitutional Law* 1 (2013).

[38] *Ibid*.

[39] Hass (ACLU), "Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions," March 27, 2014 https://www.aclu.org/blog/cell-tower-dumps-another-surveillance-technique-another-set-unanswered-questions

[40] CBC, "Police Sweeps Of Cellphone Data In 'Tower Dumps' Face Charter Challenge," http://www.huffingtonpost.ca/2016/01/14/police-sweeps-of-cellphone-data-in-tower-dumps-face-charter-challenge_n_8975432.html

[41] "Ontario Court Rules Police Orders Breached Cellphone User's Charter Rights," *The Globe and Mail,* Jan. 14, 2016 http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/court-sides-with-telecoms-in-landmark-cellphone-privacy-case/article28180968/

capable of detecting the presence and movement, even the breathing, of a person inside a building, up to fifty feet away. A unit costs about $6,000. The device was designed for the U.S. military for use in war zones like Afghanistan and Iraq.[42] However, it's tactical value and applications for domestic law enforcement are evident. The device can be used to silently and quickly scan a building before officers enter either to execute a search warrant or under exigent circumstances in which case a warrant is not required.[43] It's potentially life-saving utility for both first responders and victims in fires, natural disasters, hostage, active shooter and other such critical (and exigent) events is clear. Given it low cost and utility, widespread deployment by law enforcement agencies is expected.[44]

The Fourth Amendment implications for the use of the Range-R seem clear. Whether shooting radar rays into a home would constitute a "trespass" (*Jones, supra)* might not need to be considered, as this is clearly "exotic" sense-enhancing technology that permits the police to "pry" or "peer" into a "private place"---a residence or office---which has the highest level of Fourth Amendment protection and for which there is an unassailable reasonable expectation of privacy. The *Kyllo* decision, previously discussed, has clear application to use of the Range-R device.[45]

In a recent 10th Circuit decision out of the Kansas[46], the federal circuit court had the opportunity to pass on the use of Range R, which police used without a warrant before entering a residence to arrest a parolee at large (a fugitive). Because the authorities had ample other evidence that the fugitive was inside the residence---old fashioned "gum shoe" work like noting heightened activity on the utility meter which was in the fugitive's name, knowing he was unemployed and likely at home during the day, and even footprints in the snow outside the residence---the court did not have to pass on the lawfulness of the use of the Range R. However, the court did note the following:

> "Separately and as we alluded to earlier, the government brought with it a Doppler radar device capable of detecting from outside the home the presence of 'human breathing and movement within.' All this packed into a hand-held unit 'about 10 inches by 4 inches wide, 10 inches long.' The government admits that it used the radar before entering — and that the device registered someone's presence inside. It's obvious to us and everyone else in this case that the government's warrantless use of such a powerful

---

[42] See, "Police Use High-tech Radar to Warrantlessly Monitor People Inside Their Homes," Police State USA, Jan. 21, 2015 http://www.policestateusa.com/2015/range-r-radar/

[43] "Exigent circumstances" which would justify the warrantless entry of a home or other structure are present as a matter of law "(1) to engage in hot pursuit of a fleeing felon; (2) to prevent the imminent destruction of evidence; (3) to prevent a suspect from escaping; and (4) to prevent imminent harm to police or third parties." (*United States v. Washington*, 573 F.2d 279, 286-287 (6th Cir. 2009); accord, *United States v Daws*, 711 F.3d 725 (6th Cir. 2013).) And, in *Brigham City v. Stuart*, 547 U.S. 398 (2006), the United States Supreme Court found that exigent circumstances include the need to assist an injured occupant or prevent injury

[44] It has been reported that as of early 2015, more than 50 law enforcement agencies, including the FBI and U.S. Marshals Service, had deployed the device. CLICKOrlando, "New Police Device 'Sees' Through Walls," Jan. 20, 2015 http://www.clickorlando.com/news/new-police-device-sees-through-walls

[45] Also applicable is the U.S. Supreme Court's decision in *Florida v. Jardines*, 569 U.S. 1 (2013), in which case the Court held that police use of a trained detection dog to sniff narcotics on the front porch of a private home constituted a "search' under the Fourth Amendment, and therefore required a search warrant.

[46] *United States v. Denson*, 775 F.3d 1214 (10th Cir. 2014).

> tool to search inside homes poses grave Fourth Amendment questions. New technologies bring with them not only new opportunities for law enforcement to catch criminals but also new risks for abuse and new ways to invade constitutional rights. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 33-35 (2001) (holding that using warrantless thermal imaging to show activity inside a home violated the Fourth Amendment). Unlawful searches can give rise not only to civil claims but may require the suppression of evidence in criminal proceedings. We have little doubt that the radar device deployed here will soon generate many questions for this court and others along both of these axes. At the same time, in a criminal proceeding like ours the government is free to rely on facts gleaned independently from any Fourth Amendment violation. See *Murray v. United States*, 487 U.S. 533, 537 (1988)."

It appears evident that the courts will find that use of the Range R device, absent the existence of exigent circumstances, which could well be common, will require authorization by way of a search warrant. An officer applying for a warrant to search or enter a residence or other structure can easily include a justification and request for authorization to use the Range-R device in advance of actual entry. In fact, this will likely become a commonplace feature of search warrant applications and orders.

ShotSpotter

ShotSpotter is a gunfire locator or gunfire detection system consisting of audio or acoustic, and possibly optical and other types of sensors to detect and convey the location of gunfire or other weapon fire. ShotSpotter utilizes sophisticated acoustic triangulation technology to identify the location of gunfire from a wide range of firearms. According to the manufacturer, the system has the ability to pinpoint the location of shots fired to within 10 feet and notify police dispatchers in real time of a crime in progress. Systems used in urban settings integrate a geographic information system so the display includes a map and address location of each incident.

As reported in Wikipedia: "In public safety and law enforcement, gunshot location systems are often used in high crime areas for rapid alerts and awareness into the communications and dispatch center where the alerts are used to direct first responders to the scene of the gunfire, thus increasing arrests rates, improving officer safety, securing witnesses and evidence, and enhancing investigations, as well as in the long run deterring gun crimes, shootings and especially "celebratory gunfire" (the practice of shooting weapons in the air for fun). Additional benefits include aiding investigators to find more forensic evidence to solve crimes and provide to prosecutors to strengthen court cases resulting in a higher conviction rate."[47]

New York City has inaugurated a $1.5 million test system using more than 300 Shotspotter sensors to cover 15 square miles.[48] This is a relatively benign, if not welcome technology.[49]

---

[47] Wikipedia, "Gunfire Locator" https://en.wikipedia.org/wiki/Gunfire_locator
https://nextcity.org/daily/entry/shotspotter-installed-in-city-streetlights-ge

[48] Moraff, "Shotspotter Coming to a Streetlight Near You?, *Next City*, Oct. 7, 2015
https://nextcity.org/daily/entry/shotspotter-installed-in-city-streetlights-ge

[49] Drummond, "How Valuable a Policing Tool is Spotspotter?, *Contra Costa Times*, May 6, 2015
http://www.shotspotter.com/news/article/drummond-how-valuable-a-policing-tool-is-shotspotter , reporting that Oakland had a 26 percent reduction in gunfire per square mile since 2013.

However, deployment of the technology might have unintended consequences. Civil rights and privacy advocates, while "not losing sleep over" the technology, have concerns whether the systems will be able to detect voices.[50] In a recorded case in Oakland, ShotSpotter captured the final words of a dying man who yelled out the gunman's name. This obviously assisted the police in locating the assailant and the prosecutor in convicting him.[51]

Automated License Plate Reader (ALPR)

Automated License Plate Reader (ALPR) technology is based on fixed and mobile (in law enforcement vehicles) specialized, high-speed cameras which take digital photographs (scan) of the vehicle license plates of passing vehicles on public roadways. The system uses "character recognition software" to read the license plate's number from the scanned image The photograph is time, date and GPS location "stamped." The system is automatic and has the ability to recognize and capture thousands of vehicle license plates daily. In major metropolitan areas, these systems can scan and store hundreds of thousands of license plates per week.

The scanned license plates are downloaded automatically to a secure database for further processing and may be retained for years. Additionally, at virtually the same time the license is scanned, the system runs it against a list of known license plates associated with suspected crimes, criminal investigations, outstanding warrants and AMBER alerts---a so-called "hot list." When a "hit' is achieved, the system notifies either officers in the vehicle or at a central dispatch unit. Law enforcement can also query the stored plate scan database to assist in subsequent investigations. Of the over 70% of law enforcement agencies that employ ALPR systems, nearly all report a significant increase in crime interdiction and reduction as a direct result of the technology.[52]

There is no Fourth Amendment restraint on image capturing, scanning, storing, or cross-check features of the ALPR technology because it is capturing images in a public place where the police have a right to be and a vehicle owner has no reasonable expectation of privacy in his license plate being photographed on a public roadway.

Concerns with these systems have been raised by civil liberties groups and privacy advocates who express questions about the deployment of the system in certain communities, the capture of data that belongs to innocent persons, whether the technology allows for active surveillance and tracking of movement, and the length and depth of the retention of the data.[53]

---

[50] Stanley (ACLU), "Shotspotter CEO Answers Questions on Gunshot Detectors in Cities," May 5, 2015 https://www.aclu.org/blog/free-future/shotspotter-ceo-answers-questions-gunshot-detectors-cities

[51] Rosynsky, "Man's Dying Words Help Convict Oakland Killer," *Oakland Tribune,* Oct. 26, 2010 *http://www.insidebayarea.com/oaklandtribune/localnews/ci_16439539?source=rss*

[52] "Automated License Plate Recognition Systems: Policy and Operational guidance for Law Enforcement," International Assoc. of Chiefs of Police, March. 2012 https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf ; Newcombe, "States Start Restricting Police License Plate Readers", *Governing,* August 12, 2015 http://www.governing.com/columns/tech-talk/gov-automated-license-plate-readers-police.html

[53] ACLU, "You Are Being Tracked : How License Plate Readers Are Being Used To Record Americans' Movements," July, 2013 https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf ; Hirose (ACLU) "Documents Uncover NYPD's Vast License Plate reader Database," Jan. 25, 2016 http://www.huffingtonpost.com/mariko-hirose-/documents-uncover-nypds-v_b_9070270.html

To date, twelve states have passed legislation either restricting or regulating the operation of ALPR systems. These restrictions include limiting use to law enforcement, limiting data retention periods, imposing privacy restrictions, and requiring written policies governing system operations and data use and retention.[54]

Florida law creates a public records exemption for certain images and data obtained through the use of an ALPR system.[55] In California, the ACLU has gone to court to obtain ALPR data from law enforcement agencies in Los Angeles City and County under the state's Public Records Act. After losing in the trial the court, the ACLU took a writ to the Court of Appeal. In May 2015, the appellate court issued a published decision rejecting the ACLU's positon and finding that "investigative records" exception to the California Public Records Act covered all ALPR data and justified the City and County from withholding the records from public access. However, in July the California Supreme Court granted review in the case and it is pending in that court as of this writing.[56]

BioMetrics

Biometrics is a collective term for using human physiological characteristics as a form of identification or authentication and, in certain increasingly common applications, for access control.[57] It is estimated to be a $15 billion industry in the United States.
Fingerprints are perhaps the earliest form of biometric identification. More modernly, biometric measures have expanded to include DNA, facial recognition, scar and tattoo matching, palm print, iris scan and voice recognition. Even a person's gait can be quantified, measured and compared for identification purposes. Certain biometric measures produce highly reliable "matches," like DNA and fingerprints. Others, such as face recognition, produce "probables," chiefly of value in narrowing a set of suspects, or providing probable cause to pursue a "probable match."[58] For example, facial recognition technology can be used to identify individuals under police surveillance by matching captured biometric data with previous known biometric data, such as matching a surveillance photo with a mug shot. Computing technology has vastly increased the power of biometric identification. As for example, computerized fingerprint and

[54] National Conference of State Legislatures, "ALPR: State Statutes Regulating Their Use," Feb. 18. 2016 http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx
[55] Fla. Stat. 316.0777 (2014).
[56] *ACLU Foundation of Southern California v. Superior Court (City and County of Los Angeles),* S227106 http://appellatecases.courtinfo.ca.gov/search/case/dockets.cfm?dist=0&doc_id=2111782&doc_no=S227106
[57] For example, VISA and MasterCard are rolling out facial and fingerprint biometric authentication for security and access control for charging and payments. See, Find Biometrics Global Identify Management, "MWC 2016: A Personal Tour of MasterCard's Biometrics," Feb. 26, 2016 http://findbiometrics.com/mwc-2016-a-personal-tour-of-mastercard-biometrics-302267/
[58] See, FBI Biometric Center of Excellence, "Fingerprints and Other Biometrics," https://www.fbi.gov/about-us/cjis/fingerprints_biometrics

DNA databases can run millions of comparisons in seconds.[59] The power of biometrics has also been enhanced by improved imaging and location technologies.[60]

For law enforcement purposes and applications, the FBI Biometric Center of Excellence serves as the principal resource center and data repository, clearinghouse, and standard setter for biometric data collection, input and applications. For example, the Center has 29.3 million "searchable" photos and has plans to expand this database to 52 million.[61] State and local agencies can both contribute to and obtain assistance from this center.[62] The FBI-BCE operates under authority of 28 United States Code §534 (authorizing the collection of criminal identification data and records, and authorizing exchanging records and information with state and local agencies). The FBI collects and uses data collected only by legal means, e.g.. mugshots and fingerprints taken at post-arrest booking and evidence collected during a criminal investigation. It does not use "open sources" or social media as sources for data.[63] As part of its mission, FBI-BCE regularly accesses privacy concerns and issues Privacy Impact Assessments,[64] although this process has not been without its critics.[65]

The legality of these biometric collection, data retention, and comparison processes is clear. However, civil liberty and privacy advocates have voiced concerns over the standard less collection of biometric data, alleged indiscriminate expansion of these data bases to include nearly every citizen, and the ability to make instantaneous matches, often without sufficient standards, clear rules or oversite.[66] The *New York Times* reported on incidents in San Diego in which officers took photos of or obtained DNA samples by way of a buccal swab from individuals lawfully detained for minor offenses, and then ran the biometric data through the national database. At the time of the report the San Diego Police Department had no written policy to guide the actions of its officers. The story went on to report that over a 33 day period in January and February 2015, 26 San Diego County law enforcement agencies used facial recognition software to seek to identify individuals on more than 26,000 occasions.[67]

Clearly, these are serious concerns surrounding this expanding technology; concerns which apply to both law enforcement and private use of biometric identification. Only a handful of states have

---

[59] See, Electronic Frontier Foundation, "FBI Combines Civil and Criminal Fingerprints into One Fully Searchable Database," Sept. 15, 2015 https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-1

[60] See, Electronic Frontier Foundation, "Biometrics: Who's Watching You?," Sept. 2003 https://www.eff.org/wp/biometrics-whos-watching-you

[61] Electronic Frontier Foundation, "FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year," April 14, 2014 https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year The FBI claims an 80% "match" rate for its facial recognition technology.

[62] FBI Biometric Center of Excellence https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/

[63] FBI Biometric Specifications (BioSpecs) https://www.fbibiospecs.cjis.gov/

[64] See, e.g. FBI Records: Freedom of Information/Privacy Act, "Privacy Impact Assessment for e Guardian System," Jan. 4, 2013 https://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat

[65] See, The Crime Report, "The FBI is Watching You," Oct. 27, 2014 http://www.thecrimereport.org/news/inside-criminal-justice/2014-10-the-fbi-is-watching-you

[66] See, ACLU, "Biometrics," https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics

[67] Williams, "Facial Recognition Software Moves From Overseas Wars to Local Police," *New York Times,* Aug. 12, 2015 http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html?_r=0

passed laws regulating biometric collection and sharing by state or local agencies---Arizona, Illinois, Louisiana, Maine, Missouri, New Hampshire, Oregon, Texas and Washington[68] and currently only Illinois and Texas have laws addressing private collection of biometric data for commercial purposes.[69]. While other states can be expected to entertain legislative responses, it will fall to local officials and policy makers to adopt policies and practices that serve the interests of transparency, accountability and privacy in the applications of this technology by its law enforcement agencies.

Threat Scoring ("Beware" Software)

In January 2016 the *Washington Post* published a piece reporting on a new technological application coming into the hands of police departments---"Beware" software---which searches billions of data points, including arrest records, property records, commercial databases, Web searches and individual's social-media postings to arrive a "threat" score on an individual of interest to law enforcement. The technology can be applied to a vehicle by license number, an address or an area of a community. The *Post* article centered on the Fresno Police Department's deployment of this technology in its Real Time Crime Center, a facility that brings together a number of technologies that permits the department to see, analyze and respond to incidents as they unfold. Such centers exist in New York, Houston and Seattle.[70]

Police hail the technology as being able to provide real time information on suspects and persons of interest even as the police response is in motion. An example, cited in the *Post* article, concerned officers responding to a 911 call about a man threatening his ex-girlfriend. While patrol officers were in route, a police operator ran the individual through the Beware system and determined he had a firearm conviction and gang association,[71] so out of an abundance of caution, police called in a negotiator. But, police could employ this technology outside responding to an emerging situations, such as indiscriminately but in a targeted fashion, applying it to protesters or members of a group of concern to law enforcement.[72]

The legality of using this technology is not seriously in doubt. Nevertheless, the reaction of the privacy and civil liberties community was, to borrow an expression, fast and furious,[73] as was

---

[68] See, Ross, "Biometrics: A Developing Regulatory Landscape for a New Era of Technology," *Genomics' Law Report*, May 21, 2014 http://www.genomicslawreport.com/index.php/2014/05/21/biometrics-a-developing-regulatory-landscape-for-a-new-era-of-technology/

[69] Biometric Update.com, "States Considering Biometrics Capture Laws May Look to Illinois Privacy Laws," Aug. 5, 2015 http://www.biometricupdate.com/201508/states-considering-biometrics-capture-laws-may-look-to-illinois-privacy-laws , see, Illinois Biometric Information Privacy Act (740 ILCS 14/1, et seq.) and Texas (Bus. & Com. Code Ann. § 503.001) .

[70] Jouvenal, "The New Way Police are Surveilling You: Calculating Your Threat 'Score'," *The Washington Post*, Jan. 10, 2016 https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html

[71] Although unstated in the article, nearly every police department would have easy access to this type of information from traditional sources like state and federal criminal history data banks ("rap sheets") and internal intelligence.

[72] See, Cagle (ACLU), "This Surveillance Software is Probably Spying on #BlackLivesMatter," Dec. 15, 2015 https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter

[73] Burris, "What's Your Threat Score," *Alertnet*, Jan. 14, 2016 http://www.alternet.org/civil-liberties/whats-your-threat-score ; Stanley (ACLU), "Eight Problems with Police 'Threat" Scores," Jan. 13, 2016

that of the Fresno City Council when the system was brought to its attention and one of the councilmembers "earned" a moderate threat score based on his residential address being connected to criminal activity prior to his moving there.[74] The potential for abuse and error and the lack of "civilian" oversight and well-crafted policies are the foremost concerns. It is anticipated that state and local legislative bodies may act to regulate or guide the use of this technology in the coming months.

The ACLU has identified eight problems with the use of this technology:

- Scoring Americans in secret;
- Inaccurate data;
- Questionable effectiveness;
- Unfairness and bias;
- Potentially dangerous results;
- Unjustified government intrusion;
- First Amendment concerns;
- Mission creep.[75]

Some of these concerns can be addressed, and perhaps ameliorated, by legislation, regulation, policies, application of "best practices, and refinements in application and use based on trial and error and experience. However, others are inherent in the technology. At those conflict points, policy makers will need to balance the value of the technology to enhancing security against its potential for misuse, unintended consequences and incursions on privacy and liberty interests.

Body Worn Cameras

Police body worn camera technology ("BWC") came into national prominence in the wake of the Ferguson disturbance in August 2014.[76] This simple technology---a small wide-angle lens camera mounted on a police officer's uniform, capable of recording what is in front of the officer during "enforcement activity," and then storing that data on a server or in the Cloud for later retrieval and use, appears to have garnered support for deployment ranging from President Obama[77] to the ACLU. This wave of support was generated by the "transparency and accountability" in police-citizen interactions which this technology appears to offer. However, even before Ferguson, early deployment of BWC systems demonstrated its benefits in "civilizing" police-citizen interactions, as officers equipped with BWCs were involved in fewer police use of force incidents and faced fewer physical challenges from citizens, than those without these cameras.[78]

---

https://www.aclu.org/blog/free-future/eight-problems-police-threat-scores

[74] See, note 67, *supra*.

[75] See, Stanley (ACLU), *supra*, note 70.

[76] See, "Considering Police Body Cameras," 128 *Harvard L. Rev*. 1794 (April 10, 2015).

[77] Reuters, "Obama Calls for Body Cameras on Police," Dec. 2, 2014; Stanley (ACLU), *supra*, note 8.

[78] Farrar, Barak & Sutherland, "Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effects of Body-Worn Cameras on Police Use-of-Force," *Journal of Quantitative Criminology*, Nov 2015 (17 month study between February 2102 and July, 2103 documented that complaints against officers declined by 88 percent and use-of-force incidents declined by 60 percent for officers employing BWCs) http://www.policefoundation.org/publication/crime-mapping-analysis-news-issue-4-fall-2015/

Those who have studied the issue caution, however, that prior to deployment of BWCs, law enforcement agencies must develop and promulgate clear, detailed and transparent policies governing the equipment, training, use, storage, retention, release and disclosure, redaction and deletion and audit of BWCs and the data produced.[79]

Deployment of BWCs pose significant challenges for law enforcement agencies. Quite apart from the resource (cost) and logistic commitment for the equipment and storage and retrieval of the data, there are issues of policy development, training and administration of the technology and the data. Prosecution offices and the courts will be required to address issues going to access to and discovery of BWC data in criminal proceedings — issues which are just now emerging for prosecutors and the judiciary.

Advocates and observers alike note that BWCs promise to bring transparency, enhanced legitimacy and accountability to police conduct on the street where most encounters with citizens occur and where the vast majority of controversial incidents, including officer-involved shootings and use-of-force, occur. Experts and citizens alike believe that having a record of what happened will curb police abuse and provide a record for dealing with it when it does. For example, the data produced by BWC systems has already demonstrated expedited resolution of citizen complaints when made and resolution of lawsuits.[80]

For police and prosecutors, BWC technology is seen as making substantial contributions to the detection, identification, arrest and successful prosecution of criminal offenders, as well as the exoneration of innocent subjects. BWC data can also contribute to police training by bringing the reality of the street to the classroom.[81]

However, there are legitimate concerns about deployment of BWCs. First and foremost is the concern for citizens' privacy. Once activated, a BWC is indiscriminate in what it records, capturing everything in its "field of vision." This includes not only citizens engaged with police officers, but uninvolved bystanders and those passing by. Recording victims, who might be injured or otherwise traumatized, informants and witnesses raises both privacy and security concerns. Some experts pose the concern that the use of BWCs may act to retard crime reporting and cooperation with police officers.[82] Further, when an officer enters a home or other private place, even legitimately, the "intrusion" is made more pronounced by the fact it is being recorded.

---

[79] Brennan Center for Justice, New York University School of Law, "Police Body-Worn Camera Policies," last updated Jan. 1,2016 https://www.brennancenter.org/body-cam-city-map?splash= ; Balko, "A New Report Shows the Limits of Police Body Cameras," *The Washington Post,* Feb. 5, 2016 https://www.washingtonpost.com/news/the-watch/wp/2016/02/05/a-new-report-shows-the-limits-of-police-body-cameras/

[80] White, Michael D., "Police Officer Body-Worn Cameras: Assessing the Evidence" (Washington, DC: Office of Community Oriented Policing Services, 2014), at 11; Hayes, Jonathan; Ericson, Lars, "A Primer on Body-Worn Cameras for Law Enforcement" (U.S. Dep't of Justice, Office of Justice Programs, National Institute of Justice, 2012), at 3.

[81] *Ibid.*

[82] See, Brooks, "The Lost Language of Privacy," *New York Times,* April 14, 2015.

While use of BWCs certainly raise privacy concerns, there has been no serious challenge to their legality, either under the Fourth Amendment or common law privacy law or statutes. Police audio and video recording, even surreptitiously and without notice in public spaces, streets, and the like, is clearly within Fourth Amendment proscriptions.[83] And while there is a heightened expectation of privacy in a home or other private place, if a police officer is lawfully in a home or other private place in the legitimate discharge of his duties, recording in such circumstances does not implicate the Fourth Amendment prohibition against unreasonable search and seizure.[84] Thus, a BWC recording, even in a home or private place where an officer has a legitimate right to be under the Fourth Amendment, e.g., by reason of consent, exigent circumstances, hot pursuit, or service of a search warrant, is permissible. There does not appear to be any genuine constitutional, common law or statutory impediment or limitation to the use of BWCs, per se, so long as the officer is acting within the scope of his or her duties and the confines of the Fourth Amendment.

State legislatures have reacted swiftly to the BWC program deployment. Yet, while BWC related bills were introduced in 46 states in 2015, only four----California, Nevada, New Jersey and South Carolina---passed any measure, joining four other states with statutes already on the books---Pennsylvania, Oklahoma, Vermont, New Hampshire. One of the most controversial issues surrounding BWC programs is that of public access to the data, usually under state FOIA or Public Records laws. Many of the legislative enactments and efforts centered on this hot button issue and most acted to restrict access under these laws.[85] Civil liberties organizations, privacy advocates, the media and law enforcement have and will continue to find themselves on contending sides of this ongoing debate.[86]

Policy Considerations

Addressing many of the issues and concerns engendered by the deployment of BWCs is a matter of policy choices, administrative and management decision making, logistics and costs constraints and best practices. The technology is relatively new and model guidelines for implementation are in the developmental stages by law enforcement and justice agencies, as is the recognition of best practices. This discussion is meant to survey a number of the issues decision makers will need to address and test as use of this technology moves forward and experience is gained.

---

[83] *Lopez v. United States*, 373 U.S. 427, 437-440 (1963).

[84] *United States v. White*, 401 U.S. 745, 749 (1971) (surreptitious recording in a home where police undercover agent invited in is not a "search or seizure" under the Fourth Amendment as occupant has no reasonable expectation of privacy in that circumstance).

[85] Brown, "Nearly All States Considered Police Body Cameras in 2015, Few Enacted Laws," *Fiscal Note*, Aug. 6, 2015 https://www.fiscalnote.com/2015/08/06/nearly-all-states-considered-police-body-cameras-in-2015-few-enacted-laws/ , and see, Breitenbach, "States Grapple With Public Disclosure of Police Body-Camera Footage," *Stateline*, Sept. 22, 2015 http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/09/22/states-grapple-with-public-disclosure-of-police-body-camera-footage

[86] See, Abrams Institute (Yale Univ. Law School), "Police Body Cam Footage: Just Another Public Record,: Dec. 2015 http://isp.yale.edu/sites/default/files/publications/police_body_camera_footage-_just_another_public_record.pdf ; Stanly (ACLU), *supra*, note 7.

Equipment and Training: A department deploying BWC technology will be required to adopt procedures for acquiring and servicing equipment, as well as data storage and management. Additionally, all officers deploying the technology and their command will be required to be trained in its use, as well as legal and practical implications, evidence integrity, health and safety concerns and professional standards.

Which Officers Should Deploy BWCs: Because the primary rational for the use of BWCs is to record officer-citizen encounters on the street, deployment should be limited to uniformed patrol officers and uniformed special assignment officers (such as SWAT or crowd control) only when encounters with citizens or suspects is anticipated. Deployment considerations should comprehend that BWCs should not be used for surveillance or criminal intelligence gathering because of the privacy concerns raised by such uses. Detectives and investigators who regularly deal with victims, witnesses and informants, or who are often in homes and other private places should likewise not use BWCs because of the privacy, confidentiality and security concerns raised in such environments and under such circumstances.

How Should BWCs Be Used in the Field: Again, purpose should drive decisions regarding in-the-field use of BWCs. Continuous operation is not feasible, desirable or necessary, as it would produce mountains of unneeded and potentially intrusive and collateral data which would have to be stored and managed.

Most departments that have employed the technology charge officers with activating the BWC when contact is being made with a party while on patrol in the course of the officer's duties, thus serving the purpose behind the use of BWCs. Departments have experimented with both mandatory activation whenever contact is initiated and allowing officer discretion to activate when the officer deems it appropriate. However, mandatory activation has emerged as the "best practice," as it ensures uniform and consistent coverage and eliminates situations where the officer's judgment or intent could be second guessed for not recording. It ensures that officers are recording "everything they are supposed to." Mandatory activation additionally contributes to creating a "base line" of operation for measuring the effects of the technology within each jurisdiction. Mandatory activation enhances transparency and accountability and best serves the twin goals of protecting the public from officer misconduct and officers from false claims of misconduct.

Notice and Limits on Use in the Field: Some have suggested that giving notice to citizens that a BWC has been activated , either orally or by printed notice on the officer's uniform, is a "best practice." While not required by law and not consistently possible given the exigencies of the field, giving notice does appear to serve the goals of affecting citizen behavior toward the officer, deterring crime — particularly interference with and attacks on officers and flight —and apprizing the citizen that the encounter is being recorded so as to mitigate privacy or security concerns. If a citizen objects to being recorded, the officer can exercise his or her judgment to terminate the recording for the duration of the contact if deemed unnecessary and would foster cooperation and good relations.

When an officer enters a home, business, office or other private place, absent exigent circumstances, best practices would dictate giving notice because of heightened privacy

concerns, unless doing so would interfere with or compromise the officer's task in entering the venue. If an occupant, particularly a homeowner, objects to recording in the venue, the officer should afford particular consideration given the privacy interests at stake. This will present a difficult decision in responding to domestic violence situations where the officer is in or at a home and potentially dealing with victims, perpetrators and witnesses under highly stressful circumstances where transparency and accountability, officer and citizen protection and safety, and evidence gathering are each important and countervailing considerations. Each department might consider highly tailored and specific regulations for use of BWCs in such environments.

Likewise, BWCs should not commonly be used when encounters are with crime victims or witnesses as recording would serve little purpose other than to create a discoverable record under stressful circumstances when the victim or witness might be distraught. Further, the purpose of BWCs is not to record victim or witness statements or to serve as a substitute for proven forensic evidence gathering.

Tamper-Proof Data: There appears to be a strong consensus that data generated by BWCs — the recordings — should not be susceptible to being edited or deleted by officers in the field, "edited on the fly," or at the station. That is, all BWC-generated data should flow to the department's IT management system, which would have exclusive control of the data once it is generated in the field. This would put the data beyond manipulation by officers in the field or their immediate command.

Use of BWC Data in Report Writing and Testifying: Questions have been raised whether officers should have access to BWC data to assist in preparing incident reports and preparing for testifying in court, as that data provides a highly reliable source documenting the event subject to the report or testimony. Because incident report writing and testifying is not a memory contest, but an effort to memorialize and relate activity in the field as accurately as possible for internal and prosecution use, there does not appear to be any reason why officers should not have access to tamper-proof BWC-generated data to assist in report preparation, or to later prepare for live testimony in court.

Data Storage, Accountability, Flagging and Retention, Access, Use, Disclosure and Release, Redaction and Deletion: The biggest challenges to deploying BWC technology arise after the data is generated in the field, namely the administration of the data by the law enforcement agency once it is generated. Just as with issues concerning deployment and use of BWC technology in the field, the post-generation handling of BWC data will require the promulgation and implementation of carefully crafted, transparent and publicly reviewed and accepted policies and procedures.

Law enforcement agencies will be required to adopt and implement retention schedules for BWC data. Data that does not relate to potential criminal, civil or administrative proceedings should have a short shelf-life, measured in weeks. Data which relates to potential criminal, civil or administrative matters, including use-of-force, detention or arrest, or the commission or evidence relating to a crime, should be flagged and retained for periods consistent with the needs of the subject processes.

Each department must adopt and implement procedures to protect the integrity of the data, ensure "chain of custody" and afford the ability to audit.

Finally, agencies will be required to adopt and implement policy and procedure governing appropriate use, access, release and disclosure, redaction and destruction of BWC data. Particular consideration will have be given to use and discovery in criminal proceedings, and access by outside agencies and the press and public.

Drones[87]

Unmanned aircraft systems, otherwise known as drones, are increasingly prominent in domestic airspace as their use by hobbyists, researchers, commercial operators, local governments, and law enforcement agencies become more common. Drones are subject to regulation by the Federal Aviation Authority to ensure safety of flight, and safety of people and property on the ground. With the proliferation of domestic drone ownership and use, 2015 saw a corresponding increase in efforts to regulate drones, and to prosecute those who violate drone regulations. Approximately 45 states have considered restrictions on UAS in the last year, and local government also frequently contemplate enacting their own regulations. Yet the FAA, as a federal agency, may exercise its authority to preempt state or local regulations – whether or not they conflict with its regulations.

Congress has vested the FAA with authority to regulate airspace use, management, and efficiency, as well as air traffic control, safety, navigational facilities, and aircraft noise at its source. [88] In section 333 of the FAA Modernization and Reform Act of 2012, Congress directed the Secretary to determine whether UAS operations posing the least amount of public risk and no threat to national security could safely be operated in the national airspace system and, if so, to establish the requirements for the safe operation of those systems.

On Feb. 15, 2015, the FAA proposed a framework of regulations that defined permissible hours of flight, line-of-sight observation, altitude, operator certification, optional use of visual observers, aircraft registration and marking, and operations limits.[89] The proposed rules limit operators to flying drones during daylight hours, at speeds less than 100 mph, and below 500 feet altitude. They also require operators to maintain visual line-of-sight with the drone at all times. In December 2015, the FAA began requiring federal registration of drones to operate them in domestic airspace.[90] The FAA has determined that federal registration is the exclusive means of registering UAS for purposes of operating an aircraft in domestic airspace, which means that no

[87] This section was authored by Jordan Ferguson, Associate, Best Best & Krieger (Los Angeles). Mr. Ferguson authors "Drone on Drone" a regularly appearing feature in BBKnowledge (found at www.bbklaw.com)
[88] 49 U.S.C. §§ 40103, 44502, and 444701-44735.
[89] 14 CFR Parts 21, 43, 45, 47, 61, 91, 101, 107, and 183, available at https://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf
[90] Registration and Marking Requirements for Small Unmanned Aircraft, available at https://www.federalregister.gov/articles/2015/12/16/2015-31750/registration-and-marking-requirements-for-small-unmanned-aircraft

state or local government may impose an additional registration requirement on the operation of drones in their airspace without first obtaining FAA approval.[91]

The FAA has made clear that substantial air safety issues are raised whenever state or local governments attempt to regulate drones. The agency has expressed concern over the creation of a "patchwork quilt" of differing restrictions that could limit the flexibility of the FAA in controlling airspace and flight patterns.[92] Courts have held that a navigable airspace free from inconsistent state and local restrictions is essential to the maintenance of a safe and sound air transportation system.[93] However, courts have gone even further, indicating that, where the federal government occupies an entire field, even complimentary state and local regulations are impermissible.[94] This greatly limits the potential regulatory options available at the state and local level, and may leave prosecutors limited in the charges they can bring against drone violations

However, questions of preemption do not stop at the federal level. The FAA has laid out areas in which state and local government should avoid regulation entirely, but it has also demarcated areas where state and local laws will govern.[95] Any regulations restricting flight altitude, flight paths, or regulating the national airspace may be preempted entirely.[96] For example, the agency has specifically indicated a city ordinance banning anyone from operating drones within the city limits, within the airspace of the city, or within certain distances from landmarks would likely be preempted, or at least require consultation with the FAA prior to being adopted. Similarly, the FAA has indicated that mandating equipment or training for drones, such as geo-fencing, would likely be preempted. Courts have found that state regulation pertaining to mandatory training and equipment requirements related to aviation safety is not consistent with the federal regulatory framework.[97]

The agency has also indicated several areas that remain within state and local government police power. The FAA specifically indicates that land use, zoning, privacy, trespass, and law enforcement regulations are not subject to federal regulation and, thus, are not preempted by the FAA's regulations.[98] Among the examples the FAA has specifically indicated remain in state

---

[91] State and Local Regulations of Unmanned Aircraft Systems Fact Sheet, Federal Aviation Administration Office of the Chief Council, December 17, 2015, available at https://www.faa.gov/uas/regulations_policies/media/UAS_Fact_Sheet_Final.pdf

[92] *Ibid.*

[93] See *Montalvo v. Spirit Airlines*, 508 F.3d 464 (9th Cir. 2007); *French v. Pan Am Express, Inc*., 869 F. 2d 1 (1st Cir. 1989)

[94] See *Arizona v. United State*, ___U.S. ___, 132 S. Ct. 2492, 2502 (2012) ("Where Congress occupies an entire field … even complimentary state regulation is impermissible. Field preemption reflects a congressional decision to foreclose any state regulation in the area, even if it is parallel to federal standards"); see also *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 386-87 (1992).

[95] State and Local Regulations Fact Sheet, *supra,* note 91.

[96] Federal courts strictly scrutinize state and local regulation of overflight. *City of Burbank v. Lockheed Air Terminal*, 411 U.S. 624 (1973); *Skysign International, Inc. v. City and County of Honolulu,* 276 F.3d 1109, 1117 (9th Cir. 2002); *American Airlines v. Town of Hempstead*, 398 F. 2d 369 (2d Cir. 1968); *American Airlines v. City of Audubon Park,* 407 F. 2d 1306 (6th Cir. 1969).

[97] See, *Med-Trans Corp. v. Benton*, 581 F. Supp. 2d 721, 740 (E.D.N.C. 2008); *Air Evac EMS, Inc. v. Robinson*, 486 F. Supp. 2d 713, 722 (M.D. Tenn. 2007)

[98] See, *Skysign International, Inc. v. City and County of Honolulu¸ supra,* 276 F. 3d at 1115.

and local hands are: 1) requirements for police to obtain a warrant prior to using drones for surveillance; 2) regulations specifying that drones may not be used for voyeurism; 3) prohibitions on using drones for hunting or fishing, or to interfere with or harass an individual who is hunting or fishing; 4) prohibitions on attaching firearms or similar weapons to a drone.

Law enforcement use of drones brings with it attendant concerns about potential Fourth Amendment violations. Current jurisprudence would seem to indicate law enforcement use of drones presents no Fourth Amendment issue on its face. Two 1980's Supreme Court decisions remain the prevailing authority on law enforcement's practice of warrantless aerial surveillance. In *California v. Ciraolo*, the Court held that a police officer lawfully observed marijuana plants when he flew, at an altitude of 1,000 feet, over a suspect's backyard in a chartered plane.[99] Later, in *Florida v. Riley*, the court reached the same conclusion when officers used a helicopter to observe a marijuana grow operation in a greenhouse from 400 feet.[100] The Court held in both cases that the Fourth Amendment does not require police to obtain a warrant before observing what any other member of the public could with the naked eye—even when that observation takes place at high altitudes in the public airspace.

However, more recent cases may indicate a forthcoming shift on how we evaluate the Fourth Amendment in a world where pervasive surveillance is increasingly cheap and efficient. Decisions like *Jones* and *Riley*, and recent District and Circuit court cases on 24/7 surveillance of suspects front yards' indicate increased judicial anxiety over extended surveillance, even surveillance that takes place entirely within spaces previously considered public.[101] Though the Supreme Court has yet to address drone surveillance and its Fourth Amendment applications, these cases shed light on what that case may look like when it inevitably arises.

"Emotional Intelligence" Technology

Technology is not all high speed computers, high resolution cameras and hybrid blends of data collection and processing. There is a "soft technology" advancing to the fore in response what many view as inappropriate and unjustified incidents of police shootings and use of force. Citizens, their elected representatives, civil liberty advocates and law enforcement professionals are all pursuing measures to change the way law enforcement and community members interact to build trust and legitimacy.[102]

At a recent law enforcement conference titled "Taking Policing to a Higher Standard," held in January, 2016 in Washington D.C., some 200 police professionals, executive and experts convened to discuss policy proposals to reform police practices and procedures.[103] One of the

---

[99] *California v. Ciraolo* , *supra,* 476 U.S. 207.
[100] *Florida v. Riley*, *supra,* 488 U.S. 445.
[101] Compare, *United States v. Vargas* (E.D. Wash. Dec. 15, 2014) with *United States v. Houston* (6th. Cir. Feb. 8, 2016), *supra,* at note 24.
[102] See, President's Task Force on 21st Century Policing, May 2015 http://www.cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf ; Breitenbach, "Push for Policing Reforms Expected in Upcoming Legislative Sessions," *Stateline,* Dec. 15, 2015 http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/12/17/push-for-policing-reforms-expected-in-upcoming-legislative-sessions
[103] Lowery, "Police Chiefs Consider Dramatic Reforms to Officer Tactics, Training to Prevent So Many Shootings," *The Washington Post,* Jan. 29, 2016 https://www.washingtonpost.com/news/post-

measures discussed at this conference is loosely described as "empathy training" for police. A class entitled "Effective Interactions," train officers to deescalate situations by effectively interacting with citizens and getting their message across in a variety of different circumstances. The goal of the class is to teach and promote "emotional intelligence"---how to understand and manage one's own emotions while recognizing and respecting the feelings of others.[104] Experts hope that this type of "soft technology"/"human technology" can ameliorate the "police warrior" ethos[105] that many believe have contributed to a number of questionable or unjustified police shootings or use of force incidents. In the end, this "technology" may prove to be the most critical and successful of all in promoting both security and community trust in law enforcement.

nation/wp/2016/01/29/police-chiefs-consider-dramatic-reforms-to-officer-tactics-training-to-prevent-so-many-shootings/

[104] Winkley, "Teaching Police Empathy to Deter Use of Force," *San Diego Union Tribune*, Feb. 14, 2016 http://www.sandiegouniontribune.com/news/2016/feb/14/tp-teaching-police-empathy-to-deter-use-of-force/

[105] Stoughton, "Law Enforcement's 'Warrior' Problem" 128 Harv. L. Rev. 225 (April 15, 2015) http://harvardlawreview.org/2015/04/law-enforcements-warrior-problem/