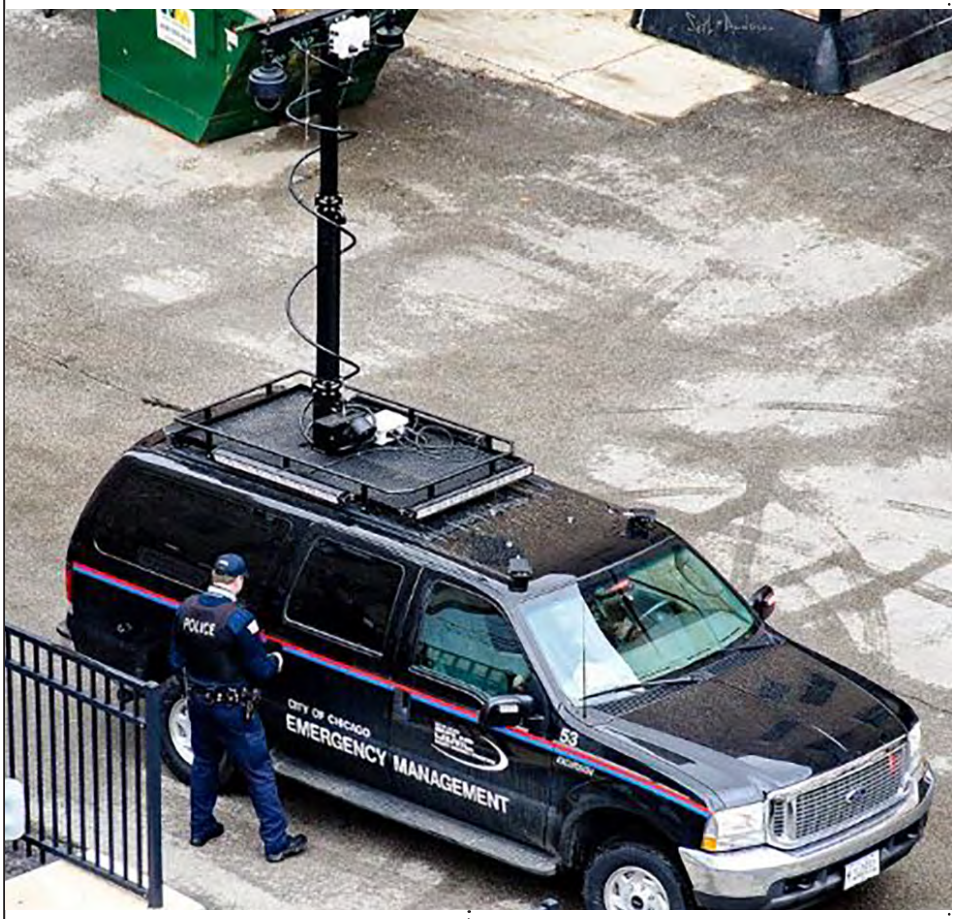
Public Safety Technologies: Big Brother and the Fourth Amendment

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



Introduction-The Evolving Collision Between Law and Technology

Technological advancements in imaging, activity and sound detection, global positioning, data collection and mining, and biometrics are rapidly being adapted to law enforcement, enhancing public safety and facilitating criminal prosecutions. In parallel with these developments, the near-universal use of portable electronic devices is exposing ever more intimate personal details to monitoring and interception. At the crossroads of these technologies are concerns for privacy, civil liberties, the limits of government power, and the contours of ordered liberty in the 21st Century.

The principal restraint on governmental intrusions into "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 what is "private" has been based on a person's subjective expectation of privacy. Recent technological advances have contorted the notion of "prying" and "privacy" at both ends of the spectrum. For example, armed with infrared detection devices, police can detect heat radiating from a home, indicating ongoing narcotics production. Is this "prying into a private place," or merely detecting heat emanating from a building?[2]

On the other hand, courts have generally found that police are entitled to search an arrestee's wallet or purse without a warrant. But what about searching a cellphone? Once this was permissible, but no longer.[3] As will be discussed, Fourth Amendment jurisprudence is in a constant race to keep up with advances in police-deployed technology, and some scholars believe that the Fourth Amendment alone cannot protect privacy from these new technologies.[4]

The Constitution is not the only bulwark against overreach. There are other sources for checks on technology-enabled police intrusions into "privacy". Restraints can originate in state legislatures.[5] Groups such as the ACLU have launched inquiries into law enforcement use of these technologies through Freedom of Information Act and Public Records Acts requests--with follow-on exposes driving changes in practices and procedures.[7] And local police agencies are responding to "civilian" oversight by developing policies which restrain use of advanced technologies.[8]

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

The Supreme Court has grappled with Fourth Amendment implications of technological advances in law enforcement for nearly a century. The progress of the law has been not been doctrinally consistent. The Court's 1928 *Olmstead* decision,[9] regarding telephone wiretaps, premised the determination of whether a "search" has occurred on the notion of physical trespass, and looked

to the place where the search was conducted. The 1967 *Katz* decision largely repudiated the "trespass" doctrine of *Olmstead* and instead focused on whether the search intruded into a place where a person had a reasonable subjective expectation of privacy.[10] However, over the last several decades, the Court reverted to sanctity for certain places, foremost the home,[11] and looked to the nature of the intrusion rather than the strict expectation of privacy, particularly when reviewing "sense enhancing" technology employed by law enforcement.

In *Kyllo* (the case previously mentioned involving thermal imaging 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 characterized this reasoning as

the "Walmart test,"[13] a particularly relevant construct when applied to commercially-available drones.[14]

Two fairly recent decisions by the Supreme Court illustrate the challenges in applying the Fourth Amendment to new technologies. *United States v. Jones*[15] questioned whether the police attaching a GPS tracking device to a vehicle, without a warrant, and use of the device to monitor the vehicle's movements on public streets for 28 days, constitutes a "search" under the Fourth Amendment. The GPS-derived data ultimately enabled police to locate a cache of 97 kilograms of cocaine and $850,000 and arrest Jones. He argued that the evidence must be suppressed. The government's argument was that under *Katz*, Jones had no reasonable expectation of privacy in the exterior of the vehicle or in locations the vehicle traveled on public roads, which made it visible to all. The government relied on one of the tenets of *Katz*: what a person knowingly exposes to the public, even in his own home or office, is not constitutionally protected.[16]

Writing for a unanimous Court, Justice Scalia impliedly rejected the government's *Katz*-based arguments, reverting to *Olmstead's* trespass-based understanding of the Fourth Amendment: "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.' "[17]

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 in determining whether, in the context of emerging technologies, a Fourth Amendment search has occurred and whether that 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]

For at least 45 years, the Court told police they could conduct a warrantless search of a person arrested, including 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 seized a cellphone from his pocket, finding evidence connecting Riley to a gang-related murder. He 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 Supreme Court in 2014. Riley's counsel argued that the 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 officer safety or material evidence--could not justify the wholesale intrusion into the vast trove of a digital data on a cellphone without a warrant.[21] Officer safety was not implicated: "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."[22]

Nor did evidentiary value override Constitutional concerns. While the Chief Justice conceded that cell phone data could be vulnerable to remote wiping, and that an officer seizing a phone might not be able to search it before the phone locked and its data became encrypted, he emphasized that cell phones differ in both a quantitative and a qualitative sense from other objects in a person's pocket:

> 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. [23]

Riley is a stark example of advances in technology bending the arc 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 had 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 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 a balancing of efficient law enforcement against the privacy rights of citizens, including movement, communications and identity, residences, and, importantly, personal effects.[25]

Cellphone searches are hardly the end of the story. Ever more innovative law enforcement technologies are emerging which will continue to challenge courts as they balance governmental interests against personal privacy rights:

Stingray—Locating Cellphones and Their Owners, in Real Time

Perhaps the most controversial surveillance technology now in the hands of the police is the Stingray, a cellular telephone surveillance device that identifies a cellphone's unique numeric identifier—its IMSI or ESN. Without any action by the phone's owner, cellphones regularly transmit

Continued on page 8



Gary Schons is a member of Best Best & Krieger's Public Policy and Ethics Compliance practice and counsels municipalities and private businesses who wish to promote public confidence in their processes. Prior to joining BB&K, he served as a deputy district attorney and senior advisor to the San Diego County District Attorney's Office, providing advice on public integrity issues to 300 deputy district attorneys in that office.

From 1976-2011, Gary was a member of the Criminal Division of the California Attorney General's Office, ultimately rising to head the Criminal Division in San Diego, where he supervised 75 attorneys who handled some 1,500 cases annually. He is a graduate of the University of San Diego School of Law, an avid cook, contributor of a dining column to the local paper and a golf and sailing enthusiast.

Public Safety Technologies Cont'd from page 7

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 locate of the phone (and suspect) with great precision, sometimes 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 $350,000 and $400,000.

Concerns over the use of the Stingray are many. Some of the 48 agencies in 20 states armed with the Stingray device are using it without a search warrant.[27] The 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, a cellphone transmits IMSI and cell site information without any activity by the user. This may well serve to distinguish Stingray 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. The bill would require state and local law enforcement to obtain a warrant before they could use Stingray devices, 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 Stingray.[31]

Although police may be interested in only the particular cellphone and location of a particular suspect, the Stingray device sweeps up *all* cellphones in the vicinity when it is operating, thus capturing data from "innocent bystanders." There do 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 California law addresses 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 Stingray to maintain operational, administrative, technical, and physical safeguards to protect information gathered from unauthorized access or disclosure. The bill further requires that the local agency make its information usage and privacy policies available in writing to the public.[33]

Cellphone Tower Dumps—Searching the Haystack to Find the Needle

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

Department of Justice 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 a search warrant. Some scholars have argued that this information is entitled to Fourth Amendment protection which should require a showing of a probable cause and be released 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" reveal vast amounts of data about 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, 2016 the judge ruled there was a breach of the Charter in "tower dump" production orders that required the two telecommunications companies to provide to 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 in use

Range-R Radar—"Seeing" Suspects Through Brick Walls

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 capable of detecting the presence and movement, even the breathing, of a person inside a building, up to 50 feet away. A unit costs about $6,000. The device was designed for U.S. military use in war zones like Afghanistan and Iraq;[42] however, its applications for domestic



Range -R Radar

law enforcement are evident. The device can be used to scan a building silently and quickly before officers enter, either to execute a search warrant or under exigent circumstances in which case a warrant is not required.[43] Its potentially life-saving utility for first responders and victims in fires, natural disasters, hostage, active shooter and other such critical events is clear. Given its low cost and utility, widespread deployment of Range-R Radar by law enforcement agencies is expected.[44]

The Fourth Amendment implications for Range-R seem clear. Whether shooting radar rays into a home would constitute a "trespass" might not need to be considered, because 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 originating in Kansas,[46] the 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 fugitive parolee. Because 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 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:

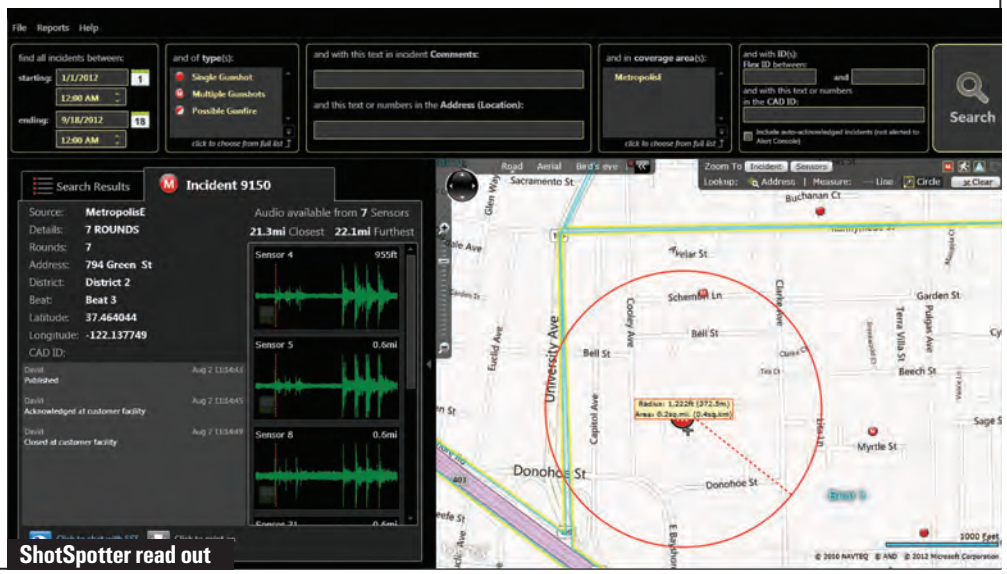
> Separately and as we alluded to earlier, the government brought with it a Doppler radar device capable of detecting from outside the home the presence of 'human breathing and movement within.' All this packed into a hand-held unit 'about 10 inches by 4 inches wide, 10 inches long.' The government admits 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 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.[47]

It appears evident that the courts will find that use of the Range-R device, absent exigent circumstances, will require a search warrant. An officer applying for a warrant to search a residence or other structure can easily include a justification for authorization to use the Range-R device. In fact, this will likely become a commonplace feature of search warrant applications and orders.

ShotSpotter—Locating the Shooter in Real Time

ShotSpotter uses sophisticated triangulation technology combined with audio, acoustic, and possibly optical and other types of sensors to detect and convey the location of gunfire. According to the manufacturer, the system can pinpoint the location of shots fired to within 10 feet and notify police dispatchers in real time. Systems used in urban settings integrate geographic data so the display includes a map and address of each incident, helping first responders rapidly reach the scene of gunfire, thus increasing arrests rates, improving officer safety, securing witnesses and evidence, and enhancing investigations—as well as in the long run deterring

Continued on page 10



ShotSpotter read out

Public Safety Technologies Cont'd from page 9

gun crimes. 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."

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]

However, deployment of the technology might have unintended consequences. Civil rights and privacy advocates, while "not losing sleep over" the technology, have concerns about whether the systems will be able to detect voices.[50] In a 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)—Linking the Car to the Crime

Automated License Plate Reader (ALPR) technology uses fixed and mobile (in law enforcement vehicles) high-speed cameras which automatically take digital photographs of passing vehicles' license plates on public roads, using character recognition software to read the plates' numbers. Each photograph is time-, date- and GPS-location "stamped." In major metropolitan areas, these systems scan and store hundreds of thousands of license plates per week, which may be stored for years.

At virtually the same time the license plate is scanned, the system runs it against a list of known plates associated with suspected crimes, criminal investigations, outstanding warrants and AMBER alerts--a so-called "hot list." Law enforcement can also query the stored plate database in subsequent investigations. Of the over 70% of law enforcement agencies that employ ALPR, nearly all report a significant increase in crime interdiction 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.

Concerns about 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]

To date, twelve states have passed legislation either restricting or regulating the operation of ALPR. 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 ALPR[55] In California, the ACLU has sued to obtain ALPR data from law enforcement under the state's Public Records Act. Although the ACLU lost in the lower courts on the grounds that that the "investigative records" exception to the California PRA covered all ALPR data; however, the California Supreme Court has granted review in the case.[56]

Biometrics—Making Anonymity Impossible

Biometrics refers to 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 original form of biometric identification, but biometric measures have now 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] Computing technology has vastly increased the power of biometric identification. As for example, computerized fingerprint and 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]

The FBI Biometric Center of Excellence serves as the principal law enforcement resource center and data repository, clearinghouse, and standard-setter for biometric data collection, input and applications. The Center has 29.3 million "searchable" photos and plans to expand this database to 52 million images.[61] State and local agencies contribute to and obtain assistance from the Center.[62] The FBI collects and uses data obtained 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, the Center 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 standardless collection of biometric data, alleged indiscriminate expansion of these databases to include nearly every citizen, and the ability to make instantaneous matches, often without sufficient standards, clear rules or oversight-.[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 governmental and private use of biometric identification. Only a handful of states have 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 respond, it will fall to local policy makers to adopt practices that serve the interests of transparency, accountability and privacy in the application of this technology.

Threat Scoring ("Beware" Software)—Combining Criminal Markers

In January 2016 the *Washington Post* published a report 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 data and individuals' social-media postings to arrive a "threat" score. The technology can be applied to a vehicle license plate number, an address or an area of a community. The *Post* article centered on the Fresno Police Department's deployment of Beware in its Real Time Crime Center, which brings together a number of technologies to follow incidents as they unfold. Such centers also 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 applying it to protesters or members of a group of concern to law enforcement.[72]

The legality of using Beware 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 that of the Fresno City Council when a councilmember "earned" a moderate threat score based on his residential address being connected to criminal activity prior to his moving there. The potential for abuse and error and the lack of "civilian" oversight and well-crafted policies are the foremost concerns. State and local legislative bodies may act to regulate or guide the use of this technology in coming months.

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

- Scoring Americans in secret;
- Inaccurate data;
- Questionable effectiveness;
- Unfairness and bias;
- Potentially dangerous results;
- Unjustified government intrusion;
- First Amendment concerns;
- Mission creep. [74]

Conclusion

Some of the concerns expressed by the ACLU and the courts can be addressed, and perhaps ameliorated, through legislation, policies, "best practices," and refinements based on trial and error and experience. However, other concerns are inherent in the technology, requiring policy makers to balance the value of enhanced security against the new technology's potential for misuse.

For municipal lawyers advising law enforcement agencies and their cities, these technologies pose significant-but not insurmountable-challenges. First, the municipal lawyer needs to be aware of the technologies, their uses and capabilities, and existing legal restraints on their use, whether constitutional or statutory. Second, the municipal lawyer needs to be sensitive to the public policy implications of these technologies, including privacy, security, public safety and legal liability. Finally, the municipal lawyer needs to be a thought-leader in helping to design policy, protocols and best practices for the responsible deployment of these technologies.

Notes

1. Katz v. United States, 389 U.S. 347(1967).
2. Kyllo v. United States, 533 U.S. 27 (2001).
3. Riley v. California, 134 S. Ct. 2473 (2014).
4. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich L. Rev. 801, 838 (2004); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 Minn. L. Rev. 1325 (2002); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 Miss. L.J. 5 (2002).
5. 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.)
6. Joseph Goldstein, *New York Police are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. Times, Feb. 11, 2016, http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=0; Greg Moran, *Cell-Tracking 'Stingray' Device was Kept Secret*, San Diego Union Trib., Feb. 13, 2016, http://www.sandiegouniontribune.com/news/2016/feb/13/cell-tracker-nondisclosure/; Matthew Cagle, *Documents Reveal Anaheim, CA Has Surprisingly Robust Surveillance Arsenal for Small City*, ACLU (Jan. 27, 2016, 6:45 PM), https://www.aclu.org/blog/free-future/documents-reveal-anaheim-ca-has-surprisingly-robust-surveillance-arsenal-small-city.
7. See Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, A Win for All*, ACLU, (last updated March 2015), https://www.aclu.org/police-body-mounted-cameras-right-policies-place-win-all.
8. Olmstead v. United States, 277 U.S. 438 (1928).
9. Katz v. United States, 389 U.S. 438 (1967).
10. *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* Kyllo v. United States, 533 U.S. 27 (2001)(use of thermal imaging to detect heat emanating from a residential marijuana grow operation required a warrant).

Continued on page 12

Public Safety Technologies Cont'd from page 11

11. Kyllo v. United States 533 U.S. at 39.
12. Christopher Slobgrin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 Minn. L. Rev. 1393 (2002).
13. 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. (Florida v. Riley, 488 U.S. 445 (1989) (police helicopter); California v. Ciraolo, 476 U.S. 207 (1986) (police in a fixed-wing airplane.) *See also* Dow Chemical Co. v. United States, 476 U.S. 277 (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).
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. 132 S.Ct. 945 (2012).
16. Katz, 389 U.S. at 351.
17. *Id.*
18. *See* Chimel v. California, 395 S.Ct. 752, 763 (1969).
19. Erin 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.
20. Riley v. California, 134 S. Ct. 2473 (2014).
21. 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, *Why Apple's CEO and the FBI are Fighting over Your Phone*, Mother Jones (Feb. 17, 2016 6:44 PM), http://www.motherjones.com/politics/2016/02/apple-ceo-tim-cook-san-bernardino-iphone.
22. Riley, 134 S. Ct. at 2473.
23. *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, 813 F.3d. 282 (6th Cir. 2016) (pole mounted camera that surveilled a rural property for 10 weeks did not require a warrant, Jones distinguished).
24. *See, e.g.*, Paul Larkin, *The Fourth Amendment and New Technologies*, Heritage Foundation Legal Memorandum #102 (Sept. 19, 2013), http://www.heritage.org/research/reports/2013/09/the-fourth-amendment-and-new-technologies.
25. Federal policy, adopted in October 2015, prohibits such use of the Stingray, effectively a wire intercept. *See*, U.S. Dep't of Justice, Use of Cell-Site Simulator Technology (2014), *available at* http://www.justice.gov/opa/file/767321/download.
26. With limited exceptions, USDOJ policy requires that federal officers obtain a search warrant based on a showing of probable cause before using the Stingray. *Id.* California's Electronic Communications Privacy Act requires officers to obtain a search warrant to use a Stingray device. *See supra* note 5. 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. N.Y. Crim. Pro. Law, Art.705 § 705.10; *see also* 18 U.S.C. § 206. *See* Goldstein *supra* note 6.
27. Smith v. Maryland, 442 U.S. 735, 744(1979).
28. Kim Zetter, *New Bill Would Force Cops to get Stingray Warrants*, Wired (November 3, 2015, 3:27 PM), 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/. 29. 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. Nathan Freed Wessler, *New Evidence Shows Milwaukee Police Hide Stingray Usage from Courts and Defense*, ACLU (Jan. 25, 2016, 1:15 PM) https://www.aclu.org/blog/free-future/new-evidence-shows-milwaukee-police-hide-stingray-usage-courts-and- defense.
30. California (SB 178 (2015)); Minnesota (SF 2466 (2014)); Utah (1HB128 (2014)); Virginia (HB 1408 (2015); Washington (HB 1440 (2015))
31. *See* Larry Greenemeier, *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. *See supra* note 5.
32. Jeff McDonald, *Police Slow to Post 'Stingray' Policies*, San Diego Union Trib., Jan. 13, 2016 http://www.sandiegouniontribune.com/news/2016/jan/13/stingray-policies/.
33. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA Today, http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ (last visited June 7, 2016).
34. Pub. L. No. 99-509, 100 Stat. 1848 (1986). U.S. Dep't of Justice, Law Enforcement Telephone Investigations Resource Guide 7 (updated Mar. 10, 2010), *available at* http://cryptome.org/isp-spy/le-tel-spy.pdf.
35. California Electronic Communications Privacy Act, Cal. Penal Code, §§ 1546 et seq. (SB 178 (2015).
36. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 J. Const. L. 1 (2013).
37. *Id.*

38. Katie Hass, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (March 27, 2014, 11:58 AM), https://www.aclu.org/blog/cell-tower-dumps-another-surveillance-technique-another-set-unanswered-questions.
38. Mike Crawley, *Police Sweeps of Cellphone Data In 'Tower Dumps' Face Charter Challenge*, CBC News (Jan 13, 2016, 5:52 PM), http://www.huffingtonpost.ca/2016/01/14/police-sweeps-of-cellphone-data-in-tower-dumps-face-charter- challenge_n_8975432.html.
40. *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/
41. *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/.
42. "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.
43. 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. Erik von Ancken, *New Police Device 'Sees' Through Walls*, Click Orlando (Jan. 20, 2015, 6:58 PM), http://www.clickorlando.com/news/new-police-device-sees-through-walls.
44. 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.
45. United States v. Denson, 775 F.3d 1214 (10th Cir. 2014).
46. *Id.*
47. Christopher Moraff, *Shotspotter Coming to a Streetlight Near You?*, Next City (Oct. 7, 2015), https://nextcity.org/daily/entry/shotspotter-installed-in-city-streetlights-ge.
48. Tammerlin Drummond, *How Valuable a Policing Tool is Spotspotter?*, East Bay Times, (May 6, 2015, 3:35 PM) http://www.eastbaytimes.com/breaking-news/ci_28063140/drummond-how-valuable-policing-tool-is-shotspotter, reporting that Oakland had a 26 percent reduction in gunfire per square mile since 2013.
49. Jay Stanley, *Shotspotter CEO Answers Questions on Gunshot Detectors in Cities*, ACLU, (May 5, 2015), https://www.aclu.org/blog/free-future/shotspotter-ceo-answers-questions-gunshot-detectors-cities.
50. Paul T. Rosynsky, *Man's Dying Words Help Convict Oakland Killer*, Oakland Tribune, Oct. 26, 2010, http://www.insidebayarea.com/oaklandtribune/localnews/ci_16439539?source=rss.
51. David J. Roberts and Meghann Casanova, Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement, International Assoc. of Chiefs of Police, March. 2012, *available at* https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf ; Tod 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.
52. *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, ACLU, https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf (last visited June 9, 2016); Mariko Hirose, *Documents Uncover NYPD's Vast License Plate reader Database*, (Jan. 25, 2016, 10:30 AM) https://www.aclu.org/blog/free-future/documents-uncover-nypds-vast-license-plate-reader-database.
53. 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.
54. Fla. Stat. 316.0777 (2014).
55. ACLU Found. of S. California v. Super. 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.
56. 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/.
57. *See* FBI Biometric Center of Excellence, *Fingerprints and Other Biometrics*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics [hereinafter FBI Biometrics] (last visited June 9, 2016).
58. *See* Jennifer Lynch, *FBI Combines Civil and Criminal Fingerprints into One Fully Searchable Database*, Electronic Frontier Foundation (Sept. 15, 2015), https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet- again-part-1.
59. *See* William Abernathy et. al., *Biometrics: Who's Watching You*, Electronic Frontier Foundation (Sept. 2003), https://www.eff.org/wp/biometrics-whos-watching-you.
60. Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, Electronic Frontier Foundation (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.
61. *See* FBI Biometrics *supra* note 57.
62. FBI Biometric Center of Excellence, *FBI Biometric Specifications (BioSpecs)*, https://www.fbibiospecs.cjis.gov/ (last visited June 9, 2016).
63. *See, e.g.*, *Privacy Impact Assessment for eGuardian System*, Fed. Bureau of Investigation (Jan. 4, 2013), https://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat.
64. *See* Adam Wisnieski, *The FBI is Watching You*, The Crime Report (Oct. 27, 2014) http://www.thecrimereport.org/news/inside- criminal-justice/2014-10-the-fbi-is-watching-you.

Continued on page 21

frastructure. Only through smart collaboration and planning can we ensure the full benefits of this technology are realized across all citizens and demographics.

Notes

1. Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles; report by U.S. DOT Volpe National Transportation Systems Center, by Anita Kim, David Perlman, Dan Bogard and Ryan Harrington, Technology Innovation and Policy Division; Preliminary Report – March 2016
2. *See* witness testimony from "Hands off: The Future of Self-Driving Cars" hearing held by Senate Committee on Commerce, Science, and Transportation; March 15, 2016.
3. Google Self-Driving Car Project; https://www.google.com/selfdrivingcar/
4. DOT/NHTSA Policy Statement Concerning Automated Vehicles" 2016 Update to "Preliminary Statement of Policy Concerning Automated Vehicles."
5. See list of enacted and pending autonomous vehicle legislation by states prepared by National Conference of State Legislators; http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx
6. Beverly Hills: Driven by Innovation; www.drivenbyinnovation.org.
7. "'Cars are parked 95% of the time'. Let's check!" by Paul Barter, posted on Reinventing Parking, Feb. 22, 2013; http://www.reinventingparking.org/2013/02/cars-are-parked-95-of-time-lets-check.html
8. Pres. Obama proposes $3.9 billion over 10-years to accelerate development and adoption of safe vehicle automation through real-world pilot projects; Jan. 14, 2016 DOT announcement.
9. Kelo v. City of New London, 545 U.S. 469 (2005).
10. Tenn. Senate Bill 1561, enacted 5/2/16 as Pub. Ch. 927.
11. United States Senate Bill S.1806; introduced 7/21/15.
12. FCC Proceeding No. 13-49 re Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure Devices in the 5 GHz Band.
13. "How Governments Can Promote Automated Driving," by Bryant Walker Smith (March 17, 2016). ML

Public Safety Technologies, Cont'd from page 13

65. *See* ACLU, *Biometrics*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics (last visited June 9, 2016).
66. Timothy Williams, *Facial Recognition Software Moves From Overseas Wars to Local Police*, N.Y. 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.
67. *See* Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, Genomics' L. Rep. (May 21, 2014) http://www.genomicslawreport.com/index.php/2014/05/21/biometrics-a-developing- regulatory-landscape-for-a-new-era-of-technology/.
68. Justin Lee, *States Considering Biometrics Capture Laws May Look to Illinois Privacy Laws*, Biometric Update.com (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 Ill. Comp. Stat. 14/1, et seq. and Tex. Bus. & Com. Code Ann. § 503.001.
69. Justin Jouvenal, *The New Way Police are Surveilling You: Calculating Your Threat 'Score'*, Wash. 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.
70. 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.
71. *See* Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU (Dec. 15, 2015), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter.
72. Sarah Burris, *What's Your Threat Score*, ALERTNET (Jan. 14, 2016), http://www.alternet.org/civil-liberties/whats-your-threat-score; Jay Stanley, *Eight Problems with Police "Threat Scores,"* ACLU (Jan. 13, 2016), https://www.aclu.org/blog/free-future/eight-problems-police-threat-scores.
73. See Williams *supra* note 66.
74. See Stanley *supra* note 72. ML

