PUBLIC LAW
CALIFORNIA LAWYERS ASSOCIATION

presents

Law Enforcement Practices & Liability Conference

The Impacts of High Technology on Policing, Ethics, and Privacy

MCLE: 2.0 Hours

Friday, May 26, 2023
3:15 p.m. - 5:15 p. m.

Speakers:

Jay Stanley, Senior Policy Analyst
ACLU Speech, Privacy, and Technology Project

Edward Medrano, President and CEO
Integrated Leadership Solutions

Jeb Brown, Senior Counsel
Liebert, Cassidy & Whitmore

Conference Reference Materials

Points of view or opinions expressed in these pages are those of the speaker(s) and/or author(s). They have not been adopted or endorsed by the California Lawyers Association and do not constitute the official position or policy of the California Lawyers Association. Nothing contained herein is intended to address any specific legal inquiry, nor is it a substitute for independent legal research to original sources or obtaining separate legal advice regarding specific legal situations.

The California Lawyers Association is an approved State Bar of California MCLE provider.

PUBLIC LAW

CALIFORNIA LAWYERS ASSOCIATION

Law Enforcement Practices and Liability Conference

The Impact of High Technology in Policing, Ethics, and Privacy

May 26, 2023

PUBLIC LAW
CALIFORNIA LAWYERS ASSOCIATION

TODAY’s PANELISTS:

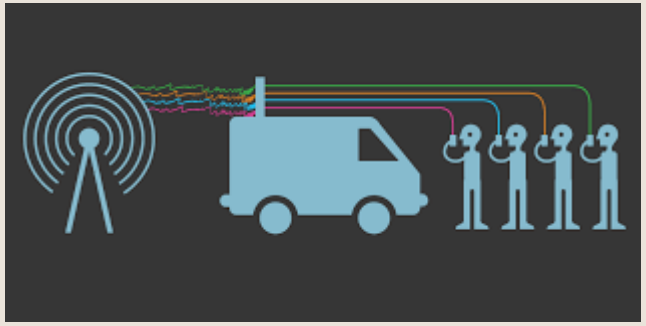
- Jeb Brown
- Jay Stanley
- Ed Medrano

LAW ENFORCEMENT TECHNOLOGY

- Video Camera Systems
  - Publicly Owned
  - Privately Owned Systems
- Drones
  - DFR
- Facial Recognition
- License Plate Readers

LAW ENFORCEMENT TECHNOLOGY

- Robots
- Tracking Systems
  - Mobile Phones
  - Cellular
  - Stingray



LEGAL AND OPERATIONAL CONSIDERATIONS

- Privacy
- 4th Amendment and other legal safeguards
- Ethics
- Policy/Practices
- Unintended consequences
- Transparency
- Community engagement
- Auditing
- Data security

PUBLIC LAW

CALIFORNIA LAWYERS ASSOCIATION

“

QUESTIONS?

"The Impacts of High Technology in Policing, Ethics, and Privacy"

The Tension Between the Right to Privacy and Police Technology

Jeb Brown, Senior Counsel, Liebert Cassidy Whitmore + Ed Medrano

Technology has continued to evolve at light speed. Technology touches all aspects of life, including policing. At a time when police budgets are tight and recruitment for police departments is challenging, technology can be used to make policing more efficient.

Technology can be used in a multitude of ways to enhance police work. It can be used as a force multiplier to allow investigations to be conducted more quickly and more accurately. It can be used to monitor events and demonstrations. It can be used to augment traffic collision investigations. However, technology can also be misused to invade privacy rights of citizens.

The Fourth Amendment governs searches and seizures. The law, as always, trails behind technology. This leaves cities and police departments to navigate the use of technology while respecting the Fourth Amendment rights of individuals. This paper will explore these issues to assist cities and police departments in balancing these competing interests.

POLE CAMERAS

Pole cameras can be typically mounted for long term use or can be a mobile, such as a pole camera on a trailer for more temporary uses. Both cameras can have the same functionality to provide opportunities for law enforcement to monitor activity at a particular location.

Pole cameras can be used to conduct remote surveillance anywhere in a city. They can be used in high crime areas or to help monitor a special event like a street fair, concert or carnival. With sufficient planning and intelligence, they can be placed to monitor marches or demonstrations. As with many types of technology, they act as a force multiplier, allowing law enforcement to observe a large area with a single officer.

Information gathered in real time is transmitted to officers on-scene. This helps in the deployment of officers, finding suspects and/or victims and allowing a more efficient use of resources. Ideally, the use of pole cameras enhances public safety.

The use of pole cameras is not without controversy. While there is no right of privacy while one is in public, courts have held that certain uses of pole cameras can have significant Fourth Amendment impacts.

In *United States v. Tuggle* (2021) 4 F. 4th 505, the Seventh Circuit considered the government's use of a pole camera. The court set the scene by stating that:

> [W]e are steadily approaching a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans. Foreseeable expansion in technological capabilities and the pervasive use of ever watching surveillance will reduce Americans' anonymity, transforming what once seemed like science fiction into fact. Constitutionally and statutorily mandated protections stand as critical

> bulwarks in preserving individual privacy vis-à-vis the government in this surveillance society. *Id*. at 509

Here, Tuggle had been previously prosecuted for conspiracy to distribute large amounts of methamphetamine. To further their investigation, the government installed three pole cameras near Tuggle's residence in order to monitor the activity at his house. The government did not obtain a warrant to place or monitor the cameras.

The three cameras were installed over a period of 13 months, from August, 2014 through September of 2015. The cameras were removed in March, 2016. The cameras recorded 24 hours a day the entire time they were installed. The cameras did not have infrared or audio capabilities. The government could pan, tilt and zoom the cameras and observe activity in real time.

The use of the cameras was successful. They captured over 100 alleged instances of deliveries of methamphetamine to Tuggle's home. Officers believed Tuggle's conspiracy distributed over twenty kilograms of pure methamphetamine.

Based on this information, officers obtained search warrants for several locations and Tuggle was indicted on multiple counts arising from his alleged conduct. Tuggle filed a motion to suppress the evidence asserting that the video obtained from the pole cameras was a warrantless search. The trial court denied his motion and an appeal followed.

The Court analyzed whether the government infringed on Tuggle's expectation of privacy. The court started with the two-part *Katz* test. (See *Katz v. United States* (1967) 389 U.S. 347.) Specifically, "[H]as the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" Tuggle bore the burden of establishing that he had a reasonable expectation of privacy in what was searched.

The Court held that the Fourth Amendment did not preclude officers from the isolated use of pole cameras on public property without a warrant. Tuggle did not erect a fence or try to shield his yard or driveway from public view. The Court stated that the expectation of privacy does not extend to what a person knowingly exposes to the public, even in his own home or office.

The Court then analyzed the more challenging question of the prolonged use of the cameras. The Court held that this use of the pole cameras did not violate the Fourth Amendment. Despite this holding, the Court had significant concerns. The Court said:

> [W]e conclude by sounding a note of caution regarding the current trajectory of Fourth Amendment jurisprudence. As technological capabilities advance, our confidence that the Fourth Amendment (as currently understood by the courts) will adequately protect individual privacy from government intrusion diminishes. Once a technology is widespread, the Constitution may no longer serve as a backstop preventing the government from using that technology to access massive troves of previously inaccessible private information because doing so will no longer breach society's newly minted expectations. With the advent of digital, cloud-based, and smart capabilities, these new technologies will seldom contravene the traditional limitations imposed by the Fourth Amendment on physical invasions. *Katz, supra*, 397 U.S. at 527.

While the use of pole cameras remains popular among law enforcement, it is clear from this opinion that courts may begin to question the use of these cameras, including the data collected from their use, when applying the Fourth Amendment in the future.

DRONES

There are as many types of drones as one can imagine. From large drones that can deliver supplies to "micro drones" that can enter a home through an open door or window, the variety is vast. These varied types of drones can assist law enforcement in a multitude of ways.

Drones provide a distinct advantage over pole cameras in that their location can be flexible. Drones can provide real time visual data in a critical incident, can be used to plan a dynamic entry for SWAT, can fly inside a structure to determine the status and location of suspects and victims, can monitor demonstrations or protests, can assist in traffic accident reconstruction or merely provide surveillance. The use of drones is limited only by the imagination.

The use of drones, given their dynamic nature, can create additional Fourth Amendment concerns. They have the capability to observe places that may be protected from public view, potentially invading a legitimate expectation of privacy.

In an en banc hearing, the Fourth District addressed some of these issues in Leaders of a *Beautiful Struggle, et. al. v. Baltimore Police Department, et. al.* (4th Cir. 2021) 2 F. 4th 330 where the Court analyzed an aerial surveillance program instituted by the Baltimore Police Department (BPD). In August 2016, the public learned that BPD was going to use planes equipped with high-tech cameras to surveil Baltimore. BPD contracted with a third party vendor, Persistent Surveillance Systems (PSS) to conduct the surveillance. Based on public opposition to the program, it was discontinued.

Three years later, after a series of townhall style meetings, the program was revived, and the City of Baltimore executed a new contract with PSS on April 1, 2020. Planes flew at least 40 hours per week and were able to capture roughly 32 square miles per image per second. The planes transmit their photographs to PSS "ground stations" where contractors use the data to "track individuals and vehicles from a crime scene and extract information to assist BPD in the investigation of Target Crimes". Target Crimes are serious crimes including homicide, armed robbery and carjacking. The data is not designed to provide real-time analysis.

Community groups filed suit seeking injunctive relief, challenging the program and alleging violations of the Fourth Amendment. By the time the matter was brought to court, the program had ended under the terms of the agreement. BPD therefore argued that the action was moot since the program had terminated.

The Fourth Circuit determined the matter was not moot because BPD retained and continued to use PSS data even though the planes were no longer flying overhead.

Turning to the Fourth Amendment merits of the case, the Court held that plaintiffs are likely to succeed and reversed the trial court's dismissal of the case. The court, in citing *Carpenter v. United States* (2018) 138 S. Ct. 2206, stated that:

Because the data is retained for 45 days— at least—it is a "detailed, encyclopedic," record of where everyone came and went within the city during daylight hours over the prior month-and-a-half. See *id*. Law enforcement

can "travel back in time" to observe a target's movements, forwards and backwards. See *id*. at 2218. Without technology, police can attempt to tail suspects, but AIR data is more like "attach[ing] an ankle monitor" to every person in the city. See *id*. "Whoever the suspect turns out to be," they have "effectively been tailed" for the prior six weeks. See *id*. ("[P]olice need not even know in advance whether they want to follow a particular individual, or when."). Thus, the "retrospective quality of the data" enables police to "retrace a person's whereabouts," granting access to otherwise "unknowable" information. See *id*.

Leaders of a Beautiful Struggle, supra, 2 F.4th at pp. 341–342. The Court further held that the surveillance was not "short-term" and transcended "mere augmentation of ordinary police capabilities." "Capturing everyone's movements outside during daytime for 45 days goes beyond that ordinary capability." *Id*. at 345. Finally, the Court stated that while not opposed to policing innovation and the use of technology to advance public safety, "the role of the warrant requirement remains unchanged as new search capabilities arise." *Id*. at 347.

This case can be applied to the use of drones. While the Supreme Court has upheld the use of flyovers without a warrant (see *California v. Ciraolo* (1986) 476 U.S. 207), the use of drones in a prolonged way that develops a library of data allowing "officers to walk back in time" may be problematic under the Fourth Amendment. Future use of drones by law enforcement will need to analyze their intended application while keeping these competing concepts in mind.

AUTOMATIC LICENSE PLATE READERS (ALPRS)

ALPRs can be mounted on vehicles or can be stationary. The government will frequently install ALPRs on police units or other vehicles. Stationary ALPRs can be used at airports, convention centers or other locations where traffic is funneled through specific locations.

The data obtained through ALPRs may then be compared to license plates of stolen vehicles or vehicles belonging to criminal suspects. That information is then used to further criminal investigations. ALPRs can also obtain vast amounts of data on where and when vehicles are present in certain locations. That data can be kept for a period of time, allowing the government to create a database of the locations of vehicles and by extension, their owners. This data then could be misused.

The California Legislature continues to attempt to regulate the use of ALPRs and more significantly, the use of the data obtained. In the last legislative session, multiple bills were introduced that would severely limit the retention period of ALPR data. Those bills mostly failed. Other bills are still pending in the Legislature addressing the sharing and/or selling of ALPR data, security regarding geolocation data, placing notice on a website when a data breach occurs and data security. Bills that were passed in 2021 and are now law (AB 474, AB 825 and AB 917) covered the security and privacy of the data.

While the Fourth Amendment does not apply to the gathering of the data, the use and retention of the data will continue to be an area where the Legislature will continue to regulate.

FACIAL RECOGNITION

Facial Recognition can be placed anywhere a camera can be placed. These cameras can be used to substitute for some security checks and in place of keys or key cards. They can also be used to identify and track a particular target, particularly where there is a network of cameras covering a wide area. Some cameras can determine emotions of targets.

Facial recognition is an emerging technology that has reliability issues. Specifically, there are issues with accuracy when attempting to identify people of color.

As seen with the cases above, the use of this type of data, particularly when collected and stored , can create Fourth Amendment issues. Many states are struggling with regulating how the technology should be used.

SHADOWDRAGON

ShadowDragon is a proprietary and new software tool. Little is known about its capabilities beyond information provided by the vendor.

ShadowDragon pulls data from social media accounts, data apps, the dark web and shopping sites like Amazon to identify a person of interest. It searches 120 different online platforms, which the company says allows it to speed up profiling work from "months to minutes". ShadowDragon also claims that its software can predict "unrest and potential violence".

It has been purchased by the U.S. Immigration and Customs Enforcement agency, the State of Michigan and the Massachusetts State Police.

Concerns regarding the use of this technology include the possible chilling effect on social media speech when there is monitoring by the government. Further, ShadowDragon can use the collected data to determine who a target may correspond with on social media. This could create a scenario where innocent people could become involved as potential suspects in a criminal investigation.

CONCLUSION

As technology continues to evolve, courts will continue to struggle to apply the Fourth Amendment to the current technologies used by the government. The courts have expressed concern that advancing technology could erode Fourth Amendment protections as we know them.

The use of this information to further public safety is critical to police agencies in light of current decreased staffing levels and tightening budgets. The Fourth Amendment will continue to play a role in the use of this technology. The best way to protect this information and allow its use in a criminal prosecution is to obtain a warrant. When the warrantless use of technology is conducted by law enforcement, there will always be a risk whether courts will allow its introduction into evidence. This tension between the law and police technology will continue to evolve as courts catch up to the various technological advances adopted by law enforcement.