LCW LIEBERT CASSIDY WHITMORE

6033 West Century Boulevard, 5th Floor
Los Angeles, California 90045
T: (310) 981-2000
F: (310) 337-0837

135 Main Street, 7th Floor
San Francisco, California 94105
T: (415) 512-3000
F: (415) 856-0306

5250 North Palm Avenue, Suite 310
Fresno, California 93704
T: (559) 256-7800
F: (559) 449-4535

401 West "A" Street, Suite 1675
San Diego, California 92101
T: (619) 481-5900
F: (619) 446-0015

400 Capitol Mall Suite 1260
Sacramento, California 95814
T: (916) 584-7000
F: (916) 584-7083

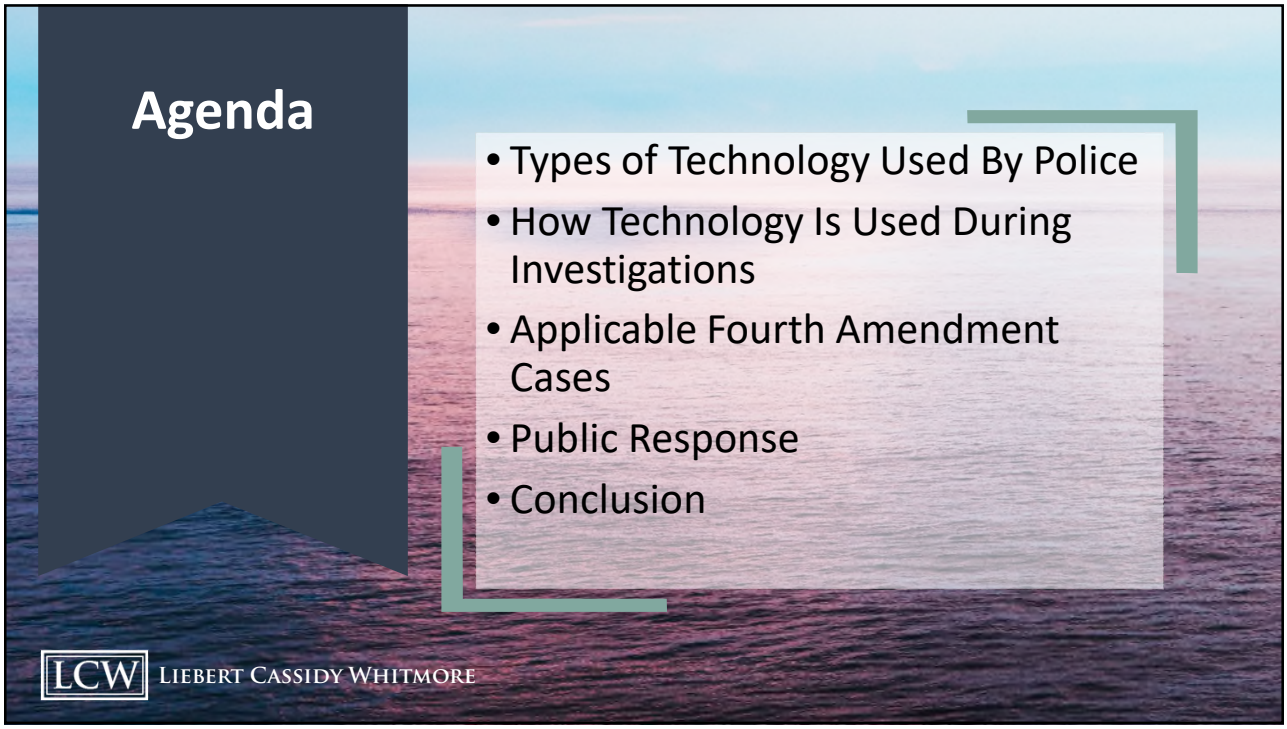
League of California Cities 2022 City Attorneys' Spring Conference

The Tension Between the Right to Privacy and Police Technology

5/4/2022

Presented by:

James E. Brown & Neil Okazaki



Introduction

- Police budgets and police staffing are under constant pressure
- Recently, crime rates have begun to rise
- The use of technology is ubiquitous in society and policing is no different
- Again, as in society, technology can be used as a force multiplier allowing agencies to do more with less
- However, the use of such technology raises serious privacy concerns that must be recognized and addressed by government

LCW LIEBERT CASSIDY WHITMORE

Technology Used

- Pole Cameras
- Drones
- Automatic License Plate Readers (ALPRs)
- Facial Recognition
- ShadowDragon

LCW LIEBERT CASSIDY WHITMORE

Pole Cameras

LCW LIEBERT CASSIDY WHITMORE

Pole Cameras

- Pole cameras can be placed in high traffic or high crime areas to monitor potential criminal activity
- Pole cameras can be a cost-effective way to deter, document and reduce crime. 24/7/365 operation.
- The most effective systems are monitored by trained staff with enough cameras to detect crimes in progress. They also integrate the technology into all law enforcement activities.
- Portable pole cameras can be quickly installed and quickly moved

LCW LIEBERT CASSIDY WHITMORE

Drones

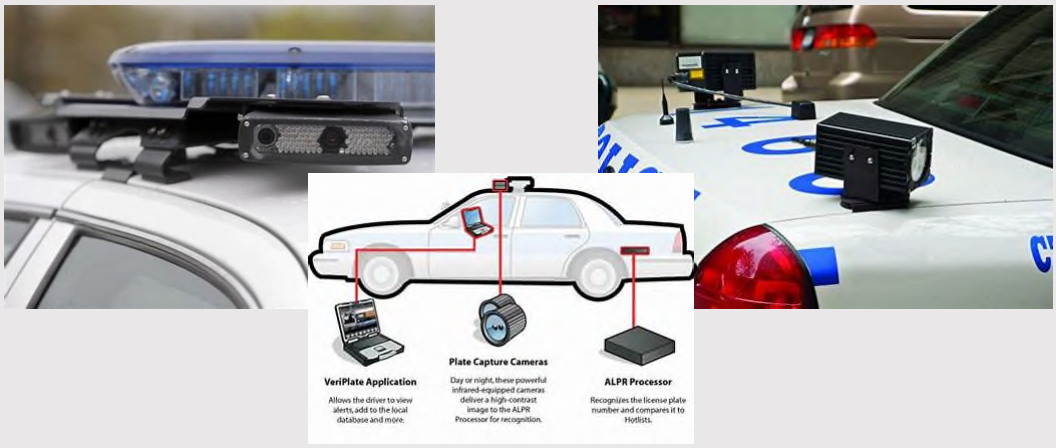

LCW LIEBERT CASSIDY WHITMORE

Drones

- Police can use drones to:
  - Document crime scenes
  - Accident reconstruction
  - Search and rescue
  - Mapping critical areas within their jurisdiction
  - Event management
  - Monitoring civil disturbances
  - Tactical operations
- Drones can be a low-cost alternative to more expensive helicopter programs
- Some agencies (Chula Vista) use drones as first responders

LCW LIEBERT CASSIDY WHITMORE

Automatic License Plate Readers



LCW LIEBERT CASSIDY WHITMORE

Automatic License Plate Readers (ALPRs)

- ALPRs capture computer-readable images that allow law enforcement to compare plate numbers against plates of stolen cars or cars driven by individuals wanted on criminal charges
- The devices are mounted on police cars, road signs or traffic lights and capture thousands of images of plates
- Vehicle Code §2413(b): California Highway Patrol may retain license plate data captured by a license plate reader (LPR) for no more than 60 days, except in circumstances when the data is being used as evidence or for all felonies being investigated, including, but not limited to, auto theft, homicides, kidnaping, burglaries, elder and juvenile abductions, Amber Alerts, and Blue Alerts.

LCW LIEBERT CASSIDY WHITMORE

Automatic License Plate Readers (ALPRs)

- The use of ALPRs data is governed by Civil Code §1798.90.5 et. seq.
- Among other things, the statutes require that operators and end users:
  - To maintain security procedures to protect ALPR information from unauthorized access, destruction, use, modification or disclosure
  - To implement a privacy policy, which must be available to the public in writing
  - The policy must include specific provisions including:
    - How the data will be used, how errors will be corrected and how long the data will be kept
- The statutes also provide for a civil action for anyone who is harmed by a violation of the statutes. They can recover damages and attorney's fees.

LCW LIEBERT CASSIDY WHITMORE

Automatic License Plate Readers (ALPRs)

- Additionally, the legislature has been very active in continuing to regulate the use of ALPRs
- In 2021-2022, twelve bills were introduced into the Senate and Assembly addressing the use of ALPRs
- Of those, five remain in committee and three have become law
- Those that became law (AB 474, AB 825 and AB 917) relate to the se and security of the ALPR data
- More specifically, these three bills extended protections to people when their ALPRs data was subject to a data breach

LCW LIEBERT CASSIDY WHITMORE

Facial Recognition

LCW LIEBERT CASSIDY WHITMORE

Facial Recognition

- Facial recognition is a digital technology that compare images obtained during criminal investigations with lawfully possessed arrest photos
- When used in combination with human analysis and additional investigation, facial recognition technology is a valuable tool in solving crimes and increasing public safety
- A facial recognition system connected to a network of cameras can automatically track an individual as they move in and out of coverage
- A facial recognition system connected to a large database of data can enable police to pinpoint a person of interest across a city of networked cameras

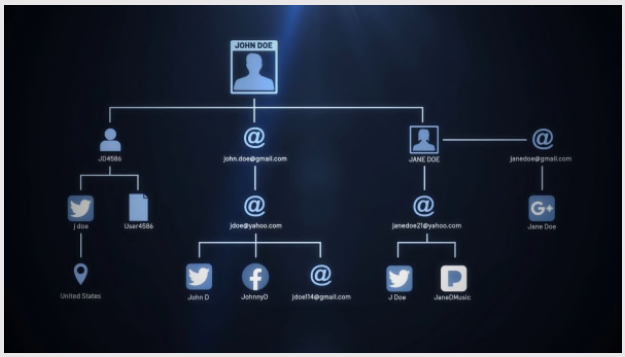
LCW LIEBERT CASSIDY WHITMORE

Facial Recognition

- Facial recognition raises multiple issues
  - Is it reliable? The technology is still relatively new and can result in false positives and false negatives.
  - Fairness concerns. 2018 study by MIT found some facial classification software misidentifies people of color at higher rates than white individuals. Algorithms have advanced since then and there have not been follow up studies to reaffirm these findings. Still, many believe those biases still exist within the technology.
  - Will it become too reliable? Will the technology create a "surveillance state" where our movements are monitored by the government 24/7? This raises general privacy concerns which are troubling.

LCW LIEBERT CASSIDY WHITMORE

ShadowDragon



LCW LIEBERT CASSIDY WHITMORE

ShadowDragon

- Searches public information from dozens of social media networks, using digital clues to identify who's behind online accounts and to visualize networks of suspected "bad actors," according to the company's website
- Suck in data from social media and other internet sources, including Amazon, dating apps, and the dark web, so they can identify persons of interest and map out their networks during investigations. By providing powerful searches of more than 120 different online platforms and a decade's worth of archives, the company claims to speed up profiling work from months to minutes. ShadowDragon even claims its software can automatically adjust its monitoring and help predict violence and unrest. Michigan police acquired the software through a contract with another obscure online policing company named Kaseware for an "MSP enterprise criminal intelligence system."

LCW LIEBERT CASSIDY WHITMORE

ShadowDragon

- ShadowDragon are part of a shadowy industry of software firms that exploit what they call "open source intelligence," or OSINT: the trails of information that people leave on the internet. Clients include intelligence agencies, government, police, corporations, and even schools.
- Investigators can run search queries for names, email addresses, phone numbers, aliases, or other information to begin to identify persons of interest, determine their physical location, ascertain their "lifestyles," and analyze their broader networks (such as friends and friends of friends)

LCW LIEBERT CASSIDY WHITMORE

ShadowDragon

- Timelines can be created to help sort out evidence and piece together clues into a broader picture of what the investigator is trying to uncover
- Physical locations can be uncovered or inferred
- This tool could have a chilling effect on speech on social media
- The tool could also link innocent people to possible criminal suspects

LCW LIEBERT CASSIDY WHITMORE

Fourth Amendment Analysis

- Fourth Amendment protects citizens against unreasonable searches and seizures
- The touchstone of Fourth Amendment analysis is whether a person has a "constitutionally protected reasonable expectation of privacy." (*Katz v. United States* (1967) 389 U.S. 347)
- Katz provided a two-part test:
  - Has the individual manifested a subjective expectation of privacy in the object of the challenged search?
  - Is society willing to recognize that expectation as reasonable? (see also *Smith v. Maryland*, (1979) 442 U.S.735)

LCW LIEBERT CASSIDY WHITMORE

California v. Ciraolo (1986) 476 U.S. 207

- Ciraolo was growing marijuana in his backyard. Police got a tip on the marijuana grow and flew over the backyard at an altitude of 1000 feet. The Supreme Court held there was no expectation of privacy in backyard when police fly overhead at 1000 feet. What a person knowingly exposes to the public, even in his own home or office, is not a subject of fourth amendment protection.
  - Since private and commercial flight is routine, any member of the public could have seen everything the officers observed
  - On these facts, the court held Ciraolo's expectation of privacy was unreasonable and not an expectation that society is prepared to honor

LCW LIEBERT CASSIDY WHITMORE

Kyllo v. U.S. (2001) 533 U.S. 27

- Agents were suspicious that Kyllo was growing marijuana in his home, which was part of a triplex. Agents used a thermal detector, which detects infrared radiation, to determine whether high intensity lights were operating at the home.
- The court held:
  - That 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 public use. This assures preservation of that degree of privacy against government that existed when the fourth amendment was adopted.

LCW LIEBERT CASSIDY WHITMORE

Kyllo v. U.S. (2001) 533 U.S. 27

- While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward
- Where, as here, the government uses a device that is not in general public use to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant

LCW LIEBERT CASSIDY WHITMORE

U.S. v. Jones (2012) 565 U.S. 400

- Jones was suspected of trafficking narcotics by the FBI
- Government applied for and obtained a warrant to use a GPS device in Washington DC. Installation required within 10 days.
- On the 11th day in Maryland, the device is installed in a public lot
- The court held:
  - That the government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search"
  - The fourth amendment protects people, not places, and is violated when the government violates the "reasonable expectation of privacy"

LCW LIEBERT CASSIDY WHITMORE

State v. Jones (2017) 903 N.W. 2d 101 (South Dakota)

- Law enforcement installed a pole camera (without a warrant) on a public street light to record defendant's activities outside of his home, beginning the same day the officers received a tip that a known drug dealer had been traveling to defendant's home to obtain drugs
- The camera recorded defendant's activities outside his home for two months, and the officers used the information gained from the camera to obtain a search warrant for defendant's home
- The officers executed the warrant and arrested defendant. Defendant moved to suppress the evidence, asserting that the officers' use of the pole camera without a warrant violated the fourth amendment.

LCW LIEBERT CASSIDY WHITMORE

State v. Jones (2017) 903 N.W. 2d 101 (South Dakota)

- The court, in determining that the placement of the pole camera was a warrantless search violating the fourth amendment, held:
  - Jones had a subjective expectation of privacy based on the amassed nature of the surveillance of his activity
  - The expectation of privacy changes when officers are able to "capture[ ] something not actually exposed to public view—the aggregate of all of [the defendant's] coming and going from the home, all of his visitors, all of his cars, all of their cars, and all of the types of packages or bags he carried and when"

LCW LIEBERT CASSIDY WHITMORE

State v. Jones (2017) 903 N.W. 2d 101 (South Dakota)

- The indiscriminate nature in which law enforcement can intrude upon citizens with warrantless, long-term, and sustained video surveillance raises substantial privacy concerns
- The warrantless use of a pole camera, specifically installed to chronicle and observe Jones's activities outside his residence from January 23 to March 19, constituted a search under the Fourth Amendment—"its use violates an expectation of privacy that society is prepared to recognize as reasonable"
- Because the use of the pole camera constituted a search, the government was required to first obtain a warrant26

LCW LIEBERT CASSIDY WHITMORE

Carpenter v. U.S. (2018) 138 S.Ct. 2206

- After the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Wireless carriers produced cell-site location information (CSLI) for petitioner Timothy Carpenter's phone.
- The government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day
- Carpenter moved to suppress the data, arguing that the government's seizure of the records without obtaining a warrant supported by probable cause violated the fourth amendment

LCW LIEBERT CASSIDY WHITMORE

Carpenter v. U.S. (2018) 138 S.Ct. 2206

- Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to fourth amendment protection
- The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the fourth amendment falls out of the picture entirely."
- The third-party doctrine does not rely solely on the act of sharing. Instead, courts considered "the nature of the particular documents sought" to determine whether "there is a legitimate 'expectation of privacy' concerning their contents."

LCW LIEBERT CASSIDY WHITMORE

Carpenter v. U.S. (2018) 138 S.Ct. 2206

- Whether the government employs its own surveillance technology or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI
- The location information obtained from Carpenter's wireless carriers was the product of a search
- When the government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements

LCW LIEBERT CASSIDY WHITMORE

Conclusion

- Case law continues to trail behind technology
- The courts struggle to determine the tension between the 4th amendment reasonable expectation of privacy and new technology
- The idea that one loses their fourth amendment protections by sharing information with a third-party continues to evolve
- When in doubt, get a warrant!

LCW LIEBERT CASSIDY WHITMORE

Thank You!

James E. Brown (Jeb)
Senior Counsel | Liebert Cassidy Whitmore
310.981.2000
JBrown@lcwlegal.com

Neil Okazaki
Assistant City Attorney | Riverside City Attorney's Office
951.826.5567
Nokazaki@riversideca.gov

LCW LIEBERT CASSIDY WHITMORE