PUBLIC SAFETY TECHNOLOGIES

International Municipal Lawyers Association 2016 Mid-Year Seminar
Washington, D.C. April 15-18, 2016

PRESENTED BY

Gary W. Schons, Of Counsel, Best Best & Krieger, San Diego
with Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy & Technology Project, Washington, D.C.

©2016 Best Best & Krieger LLP

©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 Technology v. Privacy and Private Technology

Just as the breath and power of communication and data technology in the hands of private individuals advances exponentially, so does the technology available to law enforcement to pry into both that private technology as well as our long recognized “private places.” Additionally, even traditional police methods of investigation and search and seizure threaten outsized impacts on “privacy” because of the ability to concentrate masses of data and communications in small devices.



Limits on Law Enforcement Intrusions into "Private Places"

- Fourth Amendment right against "unreasonable searches and seizures"
- Legislative enactments (federal, state and local)
- Agency policy & procedure guides
- Required accounting, reporting and audit of technology uses
- Public & media scrutiny and exposure, often based on "public record" requests, which leads to legislation, litigation and policy constraints

SCOTUS Response to Technology & the Fourth Amendment

- *Olmstead* (1928): Held a telephone wiretap was not a "search" under the Fourth Am. because there was no "physical trespass." (1934 Federal Communications Act outlawed wiretapping, but not surreptitious electronic eavesdropping.)

- *Silverman* (1961): Held police use of a "spike mike" to detect a conversation constituted a prohibited "physical trespass."

AND THEN, A "PRIVACY REVOLUTION"

- *Katz* (1967): Repudiated "trespass" doctrine and replaced it with the "reasonable expectation of privacy" test

SCOTUS DRIFT

Despite the *Katz* "reasonable expectation of privacy" test, over the last two decades of the 20th century and into the 21st century, SCOTUS' 4th Am. technology decisions expressed a "preference" for certain places, foremost the home, and looked to the nature of the law enforcement intrusion---"sense enhancing" (e.g thermal imaging) v. enhanced observation ability (overflights, surveillance cameras)

Jones (2012): The last gasp of the "Trespass Doctrine"

Police placed a GPS tracking device on a suspect's car without a warrant and monitored it on public roadways for 28 days.

Justice Scalia's majority opinion countered the government's argument that there was no "reasonable expectation of privacy" under *Katz* and held the attachment of the device to the car constituted a "trespass" in violation of the Fourth Amendment.

Jones (2012): The last gasp of the "Trespass Doctrine"

But, five other justices joined in concurring opinions by Sotomayor and Alito which held that Jones did have a "reasonable expectation of privacy" under *Katz* from such intrusive police surveillance as "societal privacy expectations" evolved in light of advancing technology. Thus, advances in technology will serve to inform the Fourth Amendment "reasonable expectation of privacy" analysis.

Riley (2014): Technology shapes "expectations of privacy"

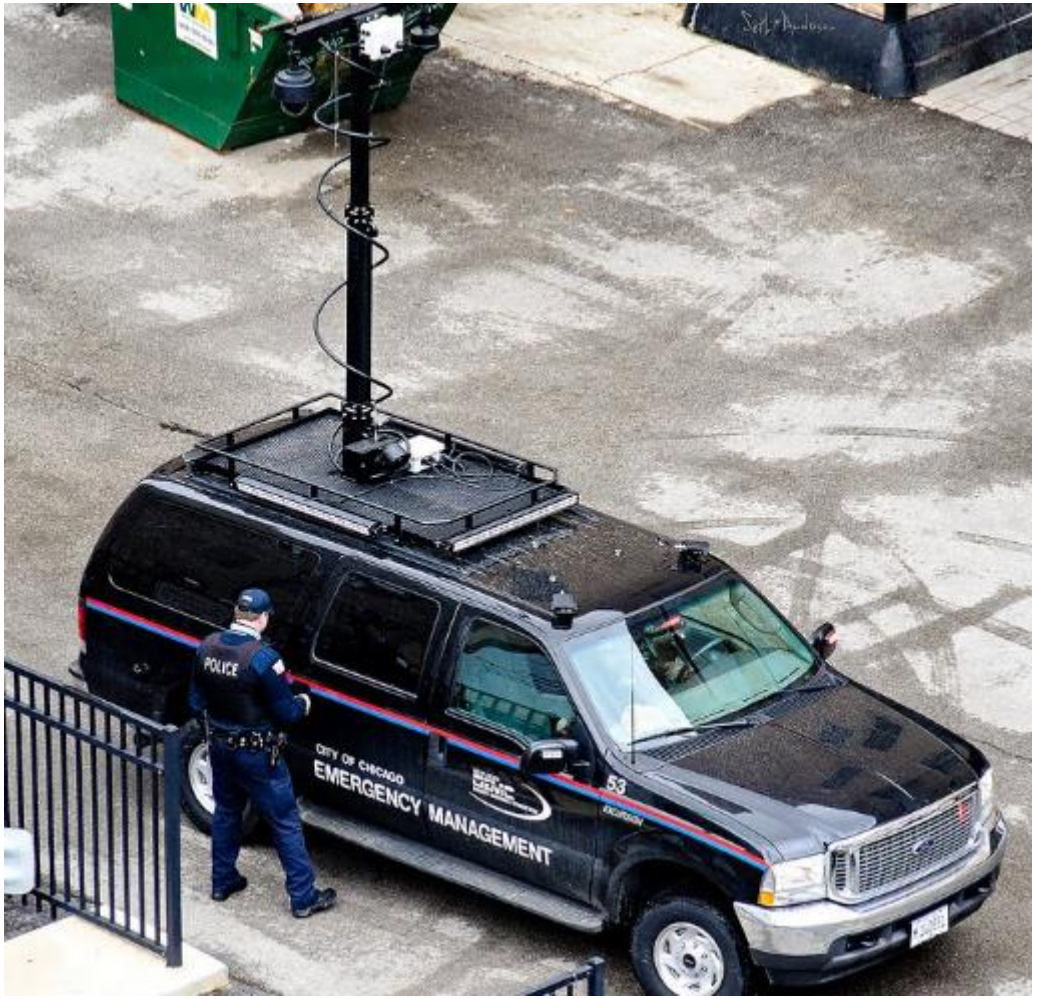
Riley, a suspected gang member, was arrested for possession of illegal weapons. Police searched his cellphone "incident to arrest" without a warrant—a long recognized exception of the warrant requirement. A unanimous opinion by CJ Roberts rejected the "search incident" exception because, compared to other common possessions, like a purse or wallet, a cellphone contains such a quality and quantity of personal information, that it merits the protection of a search warrant.

The New Paradigm for "Technology Searches"

It appears the courts will examine the *scope and nature of the information acquired regardless of its source* vs. the law enforcement justification and need for acquiring it, with a continuing preference for advance judicial authorization.

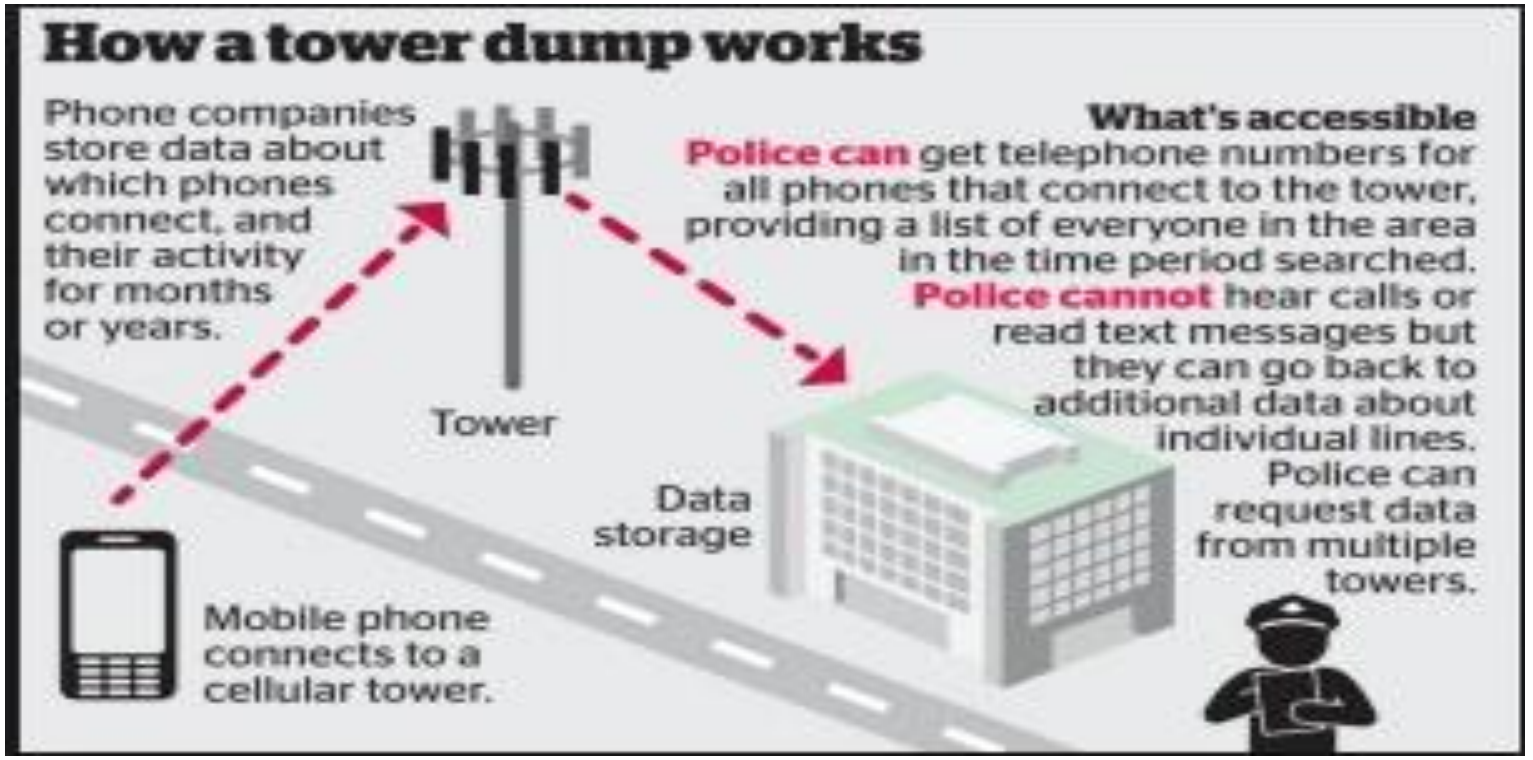
Stingray: A Cell Tower in a Box





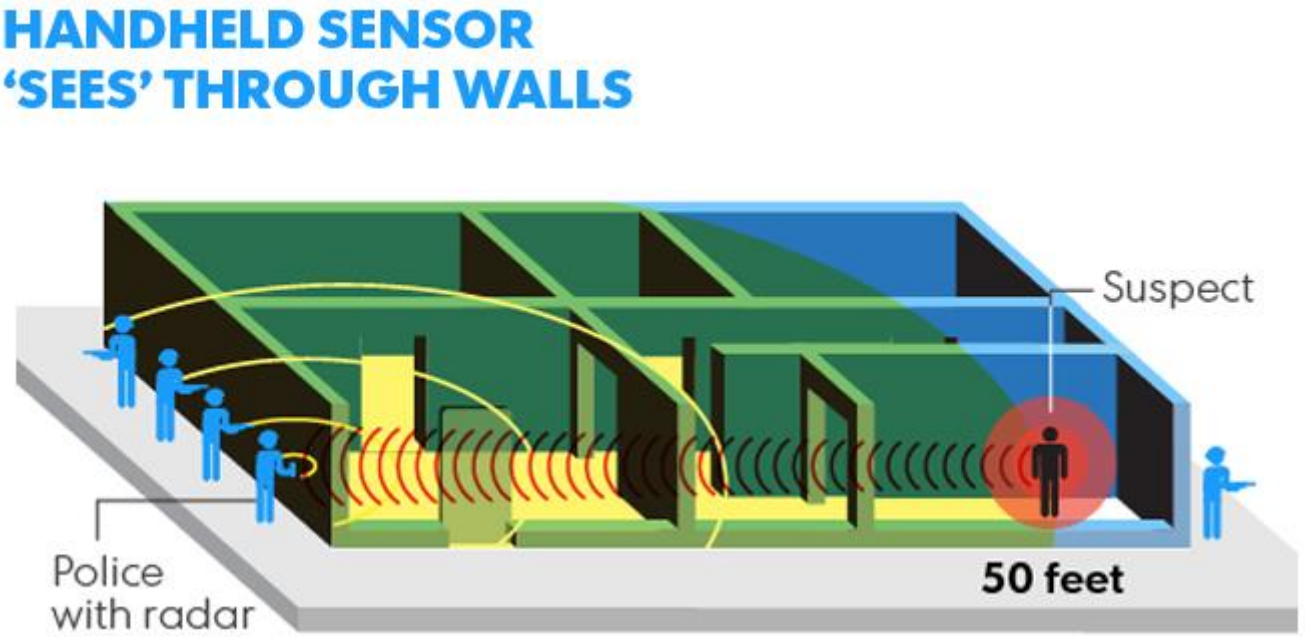
Cellphone Tower Dumps





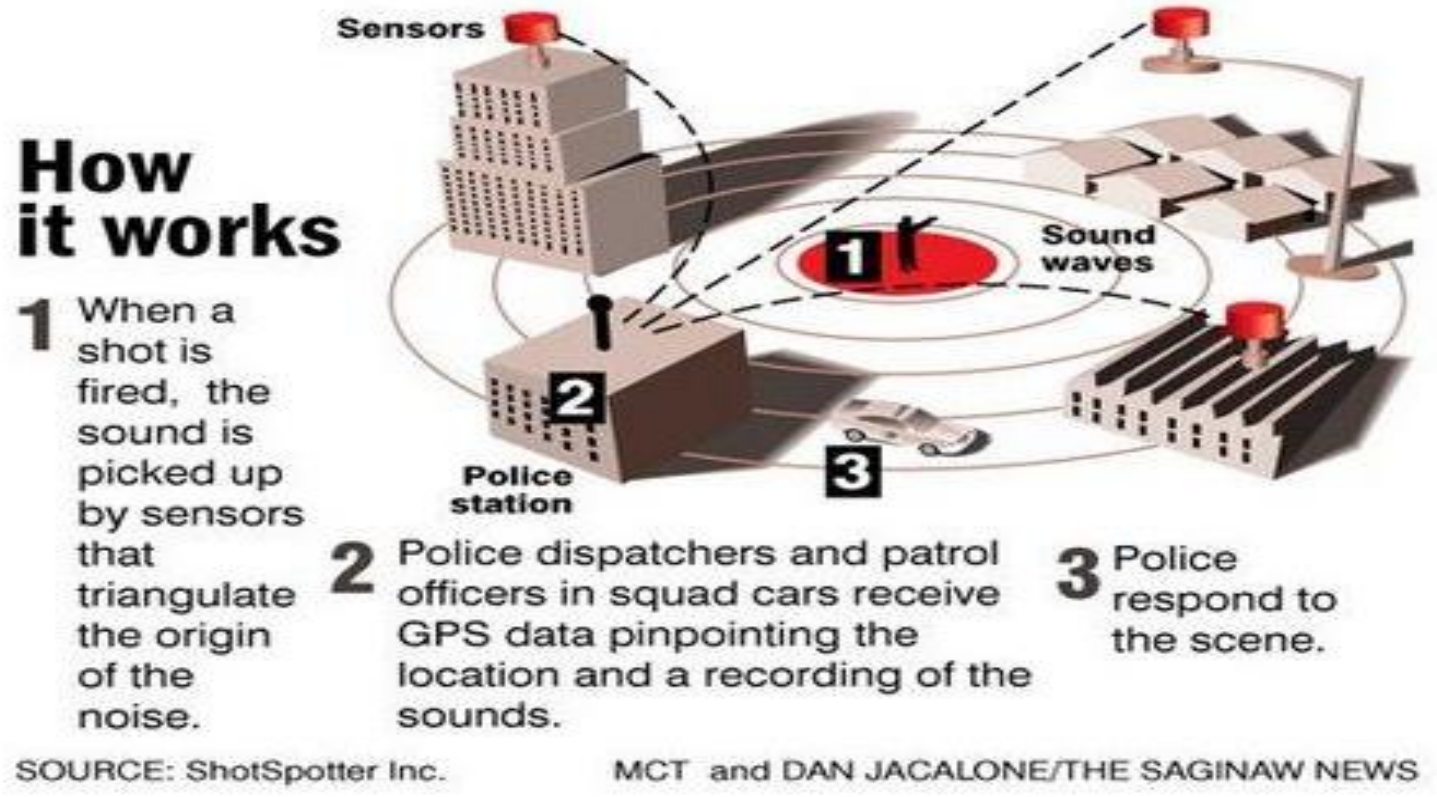
Range-R Radar





ShotSpotter





Automated License Plate Reader

"ALPR"



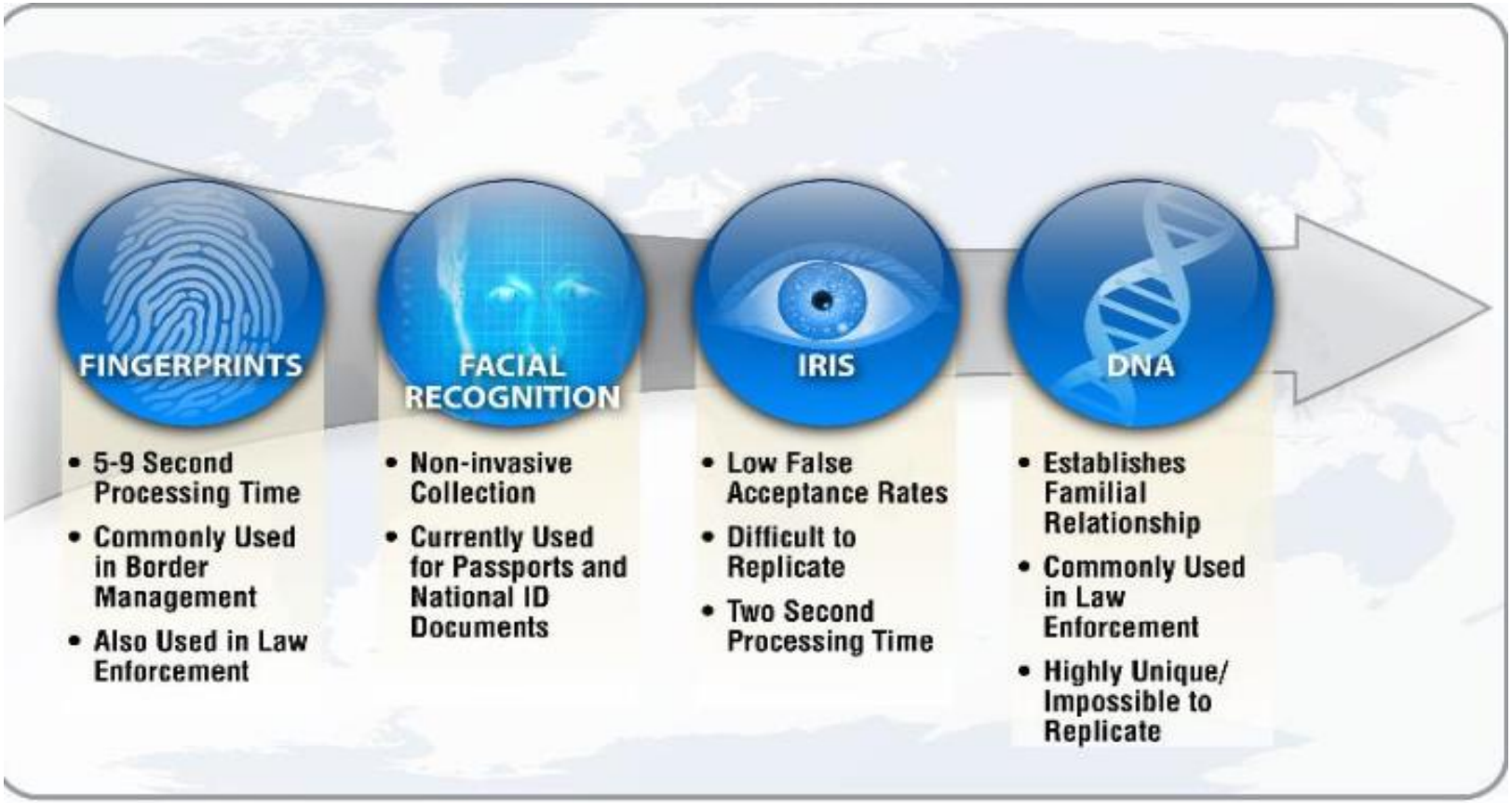






Biometrics




FINGERPRINTS
• 5-9 Second Processing Time
• Commonly Used in Border Management
• Also Used in Law Enforcement
FACIAL RECOGNITION
• Non-invasive Collection
• Currently Used for Passports and National ID Documents
IRIS
• Low False Acceptance Rates
• Difficult to Replicate
• Two Second Processing Time
DNA
• Establishes Familial Relationship
• Commonly Used in Law Enforcement
• Highly Unique/ Impossible to Replicate

Beware Software
(Threat Scoring)



Police Body Worn Cameras (BWC)







Drones





“Emotional Intelligence” Police Empathy Training









Thank you for your attention



Gary W. Schons

Of Counsel
Best Best & Krieger LLP
San Diego
Phone: 619-525-1348

Email: gary.schons@bbklaw.com
www.bbklaw.com