Emerging Technologies Impact on Police Records and the Public Records Act

California Public Records Act

- Not to be confused with Freedom of Information Act (FOIA).
- California Public Records Act is located at Cal. Gov't Code section 6250, et seq.
- The CPRA is not applicable to private companies.
- The CPRA is not the same as a subpoena to a non-litigant, civil discovery between the involved parties, or required sharing of certain information in criminal cases.

General Comments About CPRA

- Public Records Act was first enacted in 1968
- The emergence of new technologies has impacted how agencies store and respond to CPRA requests
- Emails, digital storage, the ability to instantaneously transmit large volumes of materials is a significant change since inception
- Keep in mind, the CPRA generally only requires an agency to make the information available for inspection

CPRA: What is a "Writing"

- "Writing" is not limited to a tangible document, such as a police report, but also includes video, audio, or digital records.

- A "writing" means "any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting, by electronic mail or facsimile, **and every other means of recording upon any tangible thing any form of communication or representation**, including letters, words, pictures, sounds, or symbols, or combination thereof, and any records thereby created, regardless of the manner in which the record has been stored." (Government Code section 6252(g).)

CPRA: What is a "Public Record"

- A "public record" includes "any **writing containing information** relating to the conduct of the public's business prepared, owned, **used, or retained** by any state or local agency **regardless of physical form** or characteristics." (Government Code section 6252(e).)
- Determining whether something is a "writing" should not turn on how it is stored but rather the content of the material and why the record was created.

Common Police Exemption- Investigative File- Govt. Code § 6254(f)

- EXEMPTIONS – PROTECT DOCUMENT DISCLOSURE
  - Writings related to INVESTIGATIONS BY A POLICE AGENCY (Section 6254(f).)
  - Investigatory or security files (Section 6254(f).)
  - Criminal investigations and the related records and reports would qualify as an "investigatory file."
- EXAMPLES:
  - Police Reports, Witness Statements, Security Files on suspected Terrorists.

Additional Police Exemptions to Disclosure

- DISCLOSURE NOT REQUIRED IF:
  - Endangers the safety of a witness or other person involved in the investigation.
  - Endangers the successful completion of the investigation.
  - Exempt or prohibited pursuant to federal or state law.
    - *Pitchess* motion
    - Attorney-client communications
  - Public interest keeping it confidential CLEARLY OUTWEIGHS public interest in disclosing the info. (Government Code section 6255.)

Retention of Public Records

- Government Code section 34090
- Unless otherwise provided by law, as long as the public record is more than two years old it may be destroyed.
- Still requires local governing body approval and written consent of legal counsel.
- This is the default rule so that most records older than two years may be destroyed.
- Certain exceptions to two year destruction rule apply such as birth and death certificates, real property transactions, etc.
- California Secretary of State also has a list of other local government records management guidelines.
  - www.sos.ca.gov/archives/admin-programs/local-gov-program/

One Year Retention
GC § 34090.6(a)

- Notwithstanding GC 34090, the head of a department of a city, after one year, may destroy recordings of routine video monitoring.
- After 100 days may destroy recordings of telephone and radio communications.
- Requires approval by legislative body and written consent of agency attorney
- Does not apply to evidence in any claim or pending litigation.

90 Day Retention GC § 34090.7 for Routine Video Monitoring

- Notwithstanding the other provisions of GC § 34090, routine video recordings may be destroyed after 90 days provided:
  - The agency keeps another record, such as written minutes.
  - The records are no longer required.

Body Worn Cameras/In-Car Cameras

- In-Car Cameras or Dash Cam Recordings have been around for several years
- Benefits might include better public relations
- Possible decrease in use of force incidents and citizen complaints
- Potentially puts everyone on notice to be more well behaved.

Body Worn Cameras- Steps for Implementation

- Selecting a vendor
  - Ensure proper certification with Department of Justice
  - This is because of the access to Criminal Offender Record Information (CORI) and California Law Enforcement Telecommunications System (CLETS)
  - Ensure the contract complies with best practices of state law
- Determine what equipment is required and functionality
- Creating a department policy
  - What events are to be recorded
  - When can the recordings be reviewed
  - When should it be downloaded recording, reviewing, downloading
- Storage issues
  - Cloud based storage
  - Servers and internal networks

State Law Retention Requirements Penal Code § 832.18

- Effective January 1, 2018, any law enforcement agency using body worn cameras must have a policy for storage and downloading recordings.
- Agencies must implement best practices for:
  - Downloading from camera to server or cloud based storage system
  - Establish procedures to prevent tampering, unauthorized use, or copying
  - Specify length of time to store recordings
  - Non-evidentiary data must be retained for minimum of 60 days
  - Must be keep 2 years if involves use of force, arrest, or disciplinary proceedings.
  - Records or logs of access or deletion should be retained permanently

Body Worn Cameras

- Retention Issues
  - 2 years or a shorter duration
  - State law permits destruction for non-evidentiary recordings after 60 days, but consider delays in receiving complaints or that a crime occurred
  - Costs of storage
  - Capacity will be impacted by what interactions recorded/number of officers
  - Consider impacts of on-going criminal investigations, potential lawsuits, litigation holds
- PRA application
  - Must be able to have resources to respond to PRA requests
  - Develop procedure on how to handle requests
  - How will non-privileged information be made available (i.e., send by email, copy to CD/DVD, upload to website, arrange viewing location, etc.)

Automated License Plate Readers (ALPRs)

- What do ALPR's record
  - Typically take a picture of license plate, date, time, and location
  - Picture is matched to databases to determine if stolen or wanted in connection with a crime
  - Generally less than 1% of all scans result in a hit
- Accessibility/storage issues
  - Some jurisdictions can generate millions of readings in a short time
- Public perception/ Privacy concerns

State Notification Requirements in Event of Unauthorized Disclosure

- Effective January 1, 2017, Cal. Civ. Code § 1798.29 applies to agencies with ALPR technology
  - Requires that agency must notify vehicle owners if there has been a breach of security of personal data.
  - Must have certain language (i.e., What Happened, What Information Was Involved, What We Are Doing")
  - Personal information means names, SSN, CDL, credit card information, medical information, ALPR data
  - Specifies how notice to impacted individuals must be provided
- Individual has a private cause of action against agency in the event of a security breach, up to $2500 in liquidated damages, attorney's fees, injunctive relief

ALPR Policy Requirements Cal. Civ. Code §§ 1798.90.51 and 1798.90.52

- Agencies required to maintain reasonable security practices and safeguards to protect ALPR information from unauthorized disclosure.
- Implement a written policy to ensure collection, use, maintenance, sharing, and dissemination of data is consistent with individuals' rights to privacy.
- Policy must be available for inspection to the public.
- Policy must include:
  - Purpose and use of ALPR system
  - Description of those authorized to use and access ALPR system
  - Description of measures that ALPR information is accurate and free of errors
  - Length of time data will be retained
  - Records of who and when system was accessed

ACLU v. Superior Court
3 Cal. 5th 1032 (2017)

- ACLU v. Los Angeles Sup. Ct. is a CA. Supreme Court case
  - ACLU submitted CPRA requests to LAPD and LA Sheriff Dept.
  - The scanned plates, dates, time, and location stored on confidential and restricted networks
  - Agencies refused to disclose claiming information was exempt as part of an investigative file and the need to maintain the confidentiality of the records outweighed the public's interest in disclosure
  - Due in part to a lack of a targeted inquiry or investigation, the database was too broad to be considered an investigative file
  - Court agreed though that providing dates, times, and locations of unaltered license plates threatened the privacy of the vehicle
  - Sent back to lower court to determine if there was a way to provide anonymity to private information
- Court failed to make any reference to State's laws designed to ensure privacy

International Mobile Subscriber Identity (Cell Phone trackers)

- How is information gathered
- Data retention
- Disclosure/ Exemptions
- Impacts of California Personal Electronic Communications Privacy Act to collecting data
- Since 2016, Penal Code § 1546.1 prohibits access to electronic device information absent a warrant, wire tap, or court order

Use of Social Media

- Two Main Uses of Social Media
  - Communicating department information to public
  - Use of social media to gather information or evidence
- Creation of policy to understand scope of use
  - Incidental personal use
  - Authorized IT or department staff to access, post, upload pictures
- Public agencies must be watchful and not turn social media site into a public forum
  - Balance between opinions contrasted to profane, inflammatory, off topic comments
- Impact of possible PRA request via social media site/no specified way PRA request must be made

Social Media Retention

- Retention of data
  - Is relying on social media site enough if PRA request is received
  - Length of time posts remain available to public
- Companies that monitor trending topics and related records (i.e., Geofeedia)
- Use of social media sites for investigative purposes
- Retention of investigative information
- Public perception of how law enforcement uses social media sites

Questions

Michael Fry

Office of the Sacramento City Attorney

Senior Deputy City Attorney

915 I Street, 4th Floor

Sacramento, CA 95814

(916) 808-5346

mfry@cityofsacramento.org

Kurt Wendlenner

Office of the Sacramento City Attorney

Deputy City Attorney

915 I Street, 4th Floor

Sacramento, CA 95814

(916) 808-5346

kwendlenner@cityofsacramento.org