KRASNOW SAUNDERS KAPLAN & BENINATI LLP

500 North Dearborn Street, Second Floor
Chicago, IL 60654
312.755.5700 p 312.755.5720 f
krasnowsaunders.com

Privacy Impact Assessment for the Regional Camera Project

January 7, 2015

Prepared for:

SANDAG

Acknowledgments

This Report would not be possible without the following professionals and subject matter experts who provided their valuable time, expertise, and experience.

Dan Christman
San Diego Police Department

Sara Diaz
City of El Cajon

Lloyd Muenzer
Automated Regional Justice Information System

Ed Musgrove
San Diego Metropolitan Transit System

Mike Scott
San Diego Regional Technology Partnership

Michael Swanson
San Diego Police Department

Project Staff

Katie Mugg
Automated Regional Justice Information System

Report Prepared By:

Charles A. Valente
William D. Nagel
KRASNOW SAUNDERS KAPLAN & BENINATI LLP

William D. Nagel and Charles A. Valente are the founding members of Krasnow Saunders Kaplan & Beninati, LLP's Privacy and Data Security Practice Group.

Mr. Nagel contributed to the Global Justice Information Sharing Initiative's Privacy and Civil Liberties Policy Development Guide and Implementation Templates, which helps state and local agencies evaluate the privacy implications of their data sharing initiatives. He has also prepared Privacy Impact Assessments for public safety and law enforcement agencies on a broad range of data sharing initiatives including the electronic sharing of corrections photographs, the utilization of license plate readers, and the use of facial recognition technologies to identify subjects in the field.

Mr. Valente brings more than 25 years of experience handling civil rights and other complex litigation matters as well as valuable insights into California law.

C

Contents

.

I

Introduction

The San Diego Regional Technology Partnership (RTP) is an advisory council to the San Diego Urban Area Working Group (UAWG) that recommends, plans, and implements programs that support the region's Homeland Security strategies. In 2010, RTP conducted a study to assess the number and capabilities of public surveillance cameras operating in the region. In 2011, RTP conducted a proof-of-concept pilot project and concluded that although the technology to integrate and share live video feeds was available, additional work was necessary to identify best practices for connecting camera systems and to develop policies for sharing and accessing video footage.

In 2012, RTP convened a meeting of key stakeholders, who began developing a business case document and a draft memorandum of understanding for sharing video footage.

In 2013, RTP produced the San Diego Urban Area Regional Strategic Technology Plan which recommended the enhancement of interoperable data systems and capabilities. Specifically, the Plan recommended developing a regional approach to sharing video surveillance information across multiple agencies. Based on that recommendation, the San Diego UAWG allocated Urban Area Security Initiative (UASI) funding to manage the project and develop policies related to the sharing of public surveillance footage. That funding was awarded to the Automated Regional Justice Information System (ARJIS) to conduct an assessment of how the public's privacy interests are impacted by enhancing law enforcement agencies' access to live video feeds collected by cameras owned and operated by Public Transportation Agencies (PTAs) generally.

This assessment explains, clearly and concisely, the privacy issues raised by the possible future development of a system through which law enforcement agencies would be able to access, via a secure public safety network, real-time video feeds from participating PTAs. This assessment also recommends methods by which participating PTAs and law enforcement agencies can mitigate these issues. The mitigation methods discussed below can be expanded later into formal policies and procedures with the goal of respecting the privacy rights of individuals while providing authorized users with information to help ensure public safety.

1

Part 1. Scope of the Assessment

The San Diego Urban Area Working Group (UAWG) is exploring whether to promote the development of a regional project through which law enforcement officials could access, via a secure public safety network, real-time video feeds collected by participating Public Transportation Agencies (PTAs). This assessment reviews the reasons why PTAs collect video surveillance footage, and then focuses on the privacy issues raised by the proposed sharing of PTA live feeds with law enforcement agencies.

A. Underlying Premises

This assessment is based on the following premises. If these premises change, a further assessment will be necessary.

1. **PTAs control their cameras –** PTAs determine where cameras are installed, including the camera's direction and focus. PTAs also control the pan, tilt, and zoom of cameras with those capabilities.

2. **Focus on law enforcement uses –** The following discussions focus on law enforcement agencies' use of PTA footage to investigate crimes and enforce criminal laws. This assessment does not discuss the use of video surveillance data by PTAs for purposes such as investigating or responding to civil liability claims, conducting traffic studies, or managing employees.

3. **Law enforcement agencies will not record PTA live feeds** – Law enforcement officials accessing live feeds will not record or store the footage. PTAs will remain the official repository of their own video footage. Law enforcement agencies will be required to query the archived footage stored by the PTA to obtain copies of archived footage.

4. **Existing information sharing practices remain in effect** – For several years, law-enforcement agencies have relied on private and public entities to provide video clips related to incidents under investigation (*e.g.*, bank robberies, burglaries, assaults). The following discussions are not intended to supersede these existing practices.

5. **PTA surveillance footage is not considered criminal intelligence** – The data collected by PTA surveillance cameras is only fact-based information; it is not automatically considered intelligence data. Nevertheless, if certain PTA footage is determined to have intelligence value, then law enforcement agencies should treat the footage in accordance with their internal policies implementing the regulations at 28 C.F.R. Part 23.

6. **Access to live feeds is determined at the agency level** – The leadership of each law enforcement agency determines who within the agency may access PTA live feeds.

B. Issues Not Addressed

The following issues are outside the scope of this assessment.

1. No Full-Scale Facial Recognition

Privacy advocates are concerned that, by combining surveillance footage with facial recognition software, government agencies could identify individuals to facilitate the widespread collection of each person's whereabouts into a virtual dossier. Nevertheless, facial recognition systems that attempt to identify each person captured in video footage are expensive and technologically limited in their efficiency. It is not anticipated that law enforcement agencies provided access to PTA live feeds will engage in the full-scale use of facial recognition technology for the purpose of compiling individually identifiable records of the public's whereabouts. A separate privacy impact assessment will need to be conducted if the San Diego UAWG recommends implementing the full-scale use of facial recognition technology to identify individuals appearing in PTA live feeds.

2. No Video Analytics

Video analytics (sometimes referred to as "smart video") address the problem that most surveillance systems produce far more images than is possible for human reviewers to absorb. Smart video collects and analyzes data to identify and focus on persons who act suspiciously and alert those in the viewing room. These systems rely on algorithms to profile behavior based on how people usually behave in certain environments, and then picking out those whose behavior is different from others. The major challenge, however, is anticipating the patterned behavior in a public transportation facility, where commuters carrying briefcases during the weekday rush-hour will behave differently than evening and weekend crowds attending sporting or concert events. It is not anticipated that law enforcement agencies provided access to PTA live feeds will utilize smart video technology to analyze the footage. A separate privacy impact assessment will need to be conducted if the San Diego UAWG recommends implementing video analytics to assist law enforcement agencies in their review of PTA live feeds.

3. PTA Cameras Are Not Integrated With Other Technology

Surveillance cameras can be coupled with other technologies including radio frequency identification (RFID) readers to provide a means of linking recorded images to data embedded on RFID chips, such as those included in fare cards. It is unknown whether PTAs are currently pairing RFID readers or other data collection technologies with their cameras. Nevertheless, it is not anticipated that fare card information or other similar data will be integrated into live feeds made available by PTAs.

4. No Privately-Owned Cameras Or Footage

All of the live feeds collected by PTAs are captured by cameras owned by the PTA and installed on the PTA's property, right-of-ways, and vehicles. A separate privacy impact assessment will need to be conducted if the San Diego UAWG recommends sharing live feeds from privately-owned surveillance cameras.

5. No Distinction Between Adults And Juveniles

PTA live feeds will include images of passengers under the age of 18 as well as the date and locations of their observation. The following discussions do not distinguish video footage of adults from footage containing images of juveniles.

6. No Audio Surveillance Data

Some PTAs may collect audio recordings as part of their video surveillance systems. For instance, cameras in the confined area of a train or bus operator may be equipped with a microphone to record dialogue between the operator and other PTA personnel or passengers. Although audio recordings and video footage may be useful in investigating an accident or derailment, recording conversations raises labor and employment issues as well as eavesdropping concerns. A separate privacy impact assessment will need to be conducted if the San Diego UAWG recommends that the live feeds shared with law enforcement include audio.

2

Part 2. Video Surveillance by Public Transportation Agencies

Public Transportation Agencies efficiently move vast numbers of people at low cost. PTA environments differ from office buildings or retail establishments. PTA facilities do not have either single or closely watched points of access and departure. PTA vehicles travel in predictable paths at predictable times along routes that are generally unguarded and accessible to the public. These factors make PTAs: (i) vulnerable to traditional risk management concerns such as claims for loss of property and injuries, (ii) targets for terrorism, and (iii) victims of vandalism, graffiti, and gang activity. Sharing live video feeds with law enforcement can help to ensure the public is safe, secure and resilient against terrorism and other hazards.

A. Purposes for Conducting Video Surveillance

This assessment focuses on the privacy issues raised by the proposed use of PTA live feeds by law enforcement officials. Accordingly, it assesses the original purposes for collecting the footage as well as the reasons why law enforcement officials will access and use the live feeds. As discussed in more detail below, the law enforcement purposes dovetail with the original purposes for collecting the footage.

PTA-Specific Purposes

1. **Risk management and civil investigations** – Video surveillance helps PTAs defend against fraudulent claims. For instance, cameras on transit vehicles can record whether people claiming to have been injured during an accident were actually passengers at the time of the event. Cameras at crossings and on locomotives can record whether flashing lights and gates were operable at the time of a collision.

2. **Fare collection control –** Cameras placed in entryways allow PTA staff to observe ticket vending machines and turnstiles and to assist patrons having problems with automatic fare collection systems. Such cameras also deter and assist in the apprehension of fare evaders.

3. **Deterring right-of-way trespassers** – Cameras placed along rights-of-way monitor and deter trespassers. Malevolent trespassers may try to cause a derailment by removing spikes from rails, removing nuts and bolts from rail joints, or disabling the signaling system. Even if the trespassers are innocent of any ill intentions toward the transit system, they may damage property or injure themselves.

4. **Traffic planning and management studies (vehicles and passengers) –** Cameras in stations, on platforms, and along rights-of-way collect data that PTAs use to manage risks related to overcrowding, fires, accidents, and injuries. Cameras also allow station personnel to monitor areas of dangerous crowding on platforms and escalators.

5. **Crime deterrence –** Video surveillance increases potential offenders' perceptions that they will be caught and prosecuted. Cameras also increase the public's perception of safety while using public transportation, which attracts more ridership, which further deters crime. Since vehicles parked in one spot all day are targets for theft or vandalism, cameras at parking facilities help to assure passengers that they and their vehicles are safe. Cameras in rail yards and equipment yards can protect employees working in remote locations from being victims of crime.

6. **Identifying and responding to incidents in progress** – Live video surveillance by PTAs allows them to respond, in real-time, to active shooter incidents, acts of terrorism, and bomb threats, as well as gang loitering, quality of life infractions, and vandalism. Additionally, since offenders frequently use public transportation as a means of escape, cameras allow PTA staff to monitor where fleeing suspects go after they commit crimes. Live video can also enhance first responder safety by providing information before they respond to an incident or emergency.

7. **Criminal investigations –** Surveillance video can be very beneficial for post-incident investigation by helping assess whether there were any witnesses to the incident, identify offenders, and locate discarded weapons and other evidence.

8. **Resource allocation –** Cameras are considered a force multiplier allowing one staff person to monitor more than one location.

Law Enforcement Purposes

Law enforcement officials will access, use, disseminate, and retain video footage collected by PTAs for many of the same reasons that it was originally collected, such as:

- **To deter crime –** Allowing law enforcement officials to monitor PTA live video feeds increases the number of staff available to actively monitor the surveillance cameras. The more likely a potential offender thinks that a camera is being actively monitored, the less likely he is to engage in criminal conduct at that location.

- **To identify and respond to incidents in progress** – Public transportation frequently provides offenders with a means of escaping the scene of their crime. In these situations, law enforcement officials will monitor PTA live video feeds to coordinate efforts to apprehend the offender. The live video feed also provides information valuable for formulating tactical plans and ensuring officer safety when responding to emergencies, including hostage situations, active shooter incidents, acts of terrorism, and bomb threats on PTA property and vehicles.

- **To investigate crimes** – PTA surveillance footage is a critical tool for investigators sorting out the details of an incident, especially when witnesses have left the scene, are reluctant to cooperate, or give conflicting accounts. Law enforcement officials already obtain access to archived footage on a case-by-case basis. The proposal to share live feeds with law enforcement agencies will not affect this existing practice.

- **To allocate resources –** Cameras are considered a force multiplier for law enforcement agencies by allowing the cameras to serve as replacement for patrol operations. Giving law enforcement officials access to PTA live video feeds allows the agency to assign officers to patrol areas without cameras.

B. Overview: How Video Surveillance Systems Function

Video surveillance systems consist of cameras that transmit a video signal to a specific place on a specific set of monitors. Many cameras are preprogrammed to scan an area following a set pattern (referred to as a "tour") and can also be operated remotely by human monitors or automated computer surveillance programs to focus on specific areas or activities of interest.

Systems may be actively monitored in that a person watches a series of displays in real-time, and operates the pan, tilt, and zoom controls on a number of cameras. The effectiveness of active monitoring depends on how frequently the images from each camera are displayed, the ratio of operators to video monitoring screens, and the training that operators receive on how to detect and respond to suspicious activity. "Passive" systems rely upon the retrieval of previously recorded footage, which is reviewed only after an incident is reported. Typically passive and active systems are used in combination, as few agencies have the resources to actively monitor all cameras continually.

The camera hardware is the backbone of any video surveillance system because the quality of the footage lays the foundation for its usability. To this end, cameras may be equipped with technologies that allow them to capture images beyond those that are visible to the human eye. For instance, cameras may be equipped with:

1. Built-in microphones capable of recording conversations;
2. Wide-angle lenses;
3. Magnification technology capable of capturing text on documents people are holding;
4. Motion detection and alarm recording, which can automatically focus the camera on a particular area;
5. Day/night imaging and infrared lighting technologies, which allow the camera to record in highly contrasted backlighting or total darkness; and
6. Thermal imaging technology, which creates an image using the heat energy around an object.

Agencies select which technologies to incorporate into cameras based upon the location of the camera and its intended purposes. For instance, a camera with a built-in microphone installed near the operator's cab of a PTA rail car or bus can help administrators respond more effectively when operators report an emergency. Wide-angle lenses can cover an entire area without the blind spots of traditional cameras and can reduce the number of cameras agencies need to purchase. Thermal imaging can provide a means of locating victims in the aftermath of an underground train accident or help police locate a handgun ditched in a subway tunnel by its heat signature.

Cameras are frequently connected to video management systems that record and store the footage by date, time, and location. These systems can also coordinate the wireless uploading of

footage from vehicles, stream archived video footage over the internet to authorized users, and route live surveillance feeds to first responders in case of an emergency.

C. Video Surveillance Footage is Considered Personally Identifying Information

Personally Identifiable Information ("PII") is "any information about an individual maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[1]

There is little doubt that facial images are considered personally identifiable information. Every day, people use faces to identify other people. The National Institute of Standards lists facial images as an example of PII[2] and the Driver's Privacy Protection Act categorizes photographs of people's faces as highly restricted personal information subject to the Act's highest protections.[3] California law also categorizes a digital image as personally identifying information.[4] Thus, whether accomplished through biometric identification technologies or manual data entry, surveillance footage that can link an anonymous image to a specific identified person creates privacy risks, even when the footage is collected on public property.

[1] Erika McCallister, Tim Grance, & Karen Scarfone, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST Special Publication 800-122, at 2-1 (2010), (adopting a definition of PII used by the U.S. Government Accountability Office). See also U.S. Dept. of Homeland Sec., Privacy Impact Assessment Guidance (2006) at 10-11.
[2] Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), at 2-2.
[3] See Driver's Privacy Protection Act, 18 U.S.C. §2725(4).
[4] See Cal. Penal Code § 653.2(a). Nevertheless, Cal. Streets & Highway Code § 31490(o) provides an exception that arguably may apply to some camera views.

3

Part 3. Privacy Issues Surrounding the Use of Public Video Surveillance

This Part summarizes the privacy issues created by the proposed sharing of a PTA's real-time video feeds with law enforcement agencies. The privacy concerns described below are addressed by the recommendations contained throughout the remainder of this report.

A. Expectations of Privacy in Public Spaces

The personal habits of daily life extend into public spaces. For instance, people use public transportation, streets, and sidewalks to travel to psychiatrist offices, reproductive health centers, Alcoholics Anonymous meetings, religious facilities, book stores, and political meetings. Additionally, people have private conversations with each other in crowded restaurants or while walking in the park. People read books and write in journals while sitting on public benches or riding the bus or train. The public may not reasonably expect that these types of behaviors can be captured by a public surveillance system.

Mitigation of Expectation Risks

Expectation concerns are addressed through public notice. PTAs typically notify the public when they utilize video surveillance by posting signs in areas and on vehicles where surveillance cameras are in use. The deployment of visible cameras also provides notice that video surveillance is being conducted. There is a risk that members of the public may not see the notice signage or the cameras; this can be mitigated by publishing a privacy impact assessment report that discloses the PTA's use of surveillance cameras to inform the riding public's privacy expectations while using public transportation.

Significantly, PTA cameras are deployed only on property and right-of-ways operated by the PTA and therefore do not record an individual's ultimate destination. Additionally, the cameras deployed on PTA buses and trains are generally incapable of recording the text that passengers read or write.

B. Potential Chilling Effects of Video Surveillance

Surveillance is the watching, listening to, or recording of an individual's activities.[5] The public has less confidence in its freedom to act, speak, and associate with other people or groups when it is being watched, especially by government agencies. The privacy risk of increased video surveillance is that it can be used as a tool of social control: the mere possibility of observation can make people uncomfortable and cause them to alter their behavior through self-censorship.[6]

[5] Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 490 (Jan. 2006).
[6] A Taxonomy of Privacy, 154 U. Pa. L. Rev. at 493.

For instance, a couple may choose not to kiss in public, even if they are alone, because they are not sure whether they are being watched by surveillance cameras.[7] The surveillance may also cause people to avoid monitored public places due to concerns that their presence could draw the attention of law enforcement.[8] This effect is problematic because many people cannot simply choose to avoid using public transportation either because they have no other means of transportation or live near its stations or right-of-ways.

Chilling effects of surveillance could extend to private behaviors such as selecting what clothing to wear. For example, a study of British video surveillance systems found that operators focused on subjects who wore garments thought to be indicative of the wearer's criminal intent, especially hats:

> [Camera operators] know that hats can potentially deprive them of recording a clear image of a person's face. Knowing this, they act on the assumption that citizens do as well. Operators believe they have a right to surveille any person's face who appears in their territory. Anyone who supports a visible means of denying them this opportunity immediately places himself in the category of persons of questionable intent and worthy of extended surveillance.[9]

Another study found that people wearing uniforms were routinely exempt from targeting.[10] The power of surveillance as a tool for social control, and policies to mitigate these risks, are related to the risk of discriminatory surveillance.

Mitigation of Chilling Effects

The degree of a surveillance system's chilling effect depends upon the types of information it collects, how the data will subsequently be utilized, and how long it will be stored. PTAs generally implement video surveillance systems for the purposes identified in Part 2. Although there may be some chilling effects surrounding the sharing of PTA live feeds with law enforcement, the development and implementation of policies regulating participating law enforcement agencies' access, use, dissemination, and retention of the footage discussed below can reduce those effects.

---

[7] Jeffrey Rosen, Being Watched: A Cautionary Tale for a New Age of Surveillance, New York Times Magazine (October 7, 2001).

[8] The United States Supreme Court has stated that "an individual's decision to remain in a public place of his choice is as much a part of his liberty as the freedom of movement inside frontiers that is a part of our heritage[.]" City of Chicago v. Morales, 527 U.S. 41, 53-4 (1999) (internal quotation marks omitted).

[9] Clive Norris & Gary Armstrong, CCTV And The Social Structuring Of Surveillance, Crime Prevention Studies, Vol. 10, at 167 (1998).

[10] Adrienne Isnard, Can Surveillance Cameras Be Successful In Preventing Crime And Controlling Anti-Social Behaviours?, Australian Institute of Criminology, at 13 (2001).

C. Equal Protection and Discrimination in Surveillance

Video surveillance systems that are actively monitored and controlled create a risk that the cameras will not record the public equally. For instance, a study conducted to discover who it is that is watched by camera operators found:[11]

- Men were nearly twice as likely as women to be targeted for observation than their presence in the population would suggest;
- 65% of teenagers, compared with 21% of those aged over 30, were targeted for no obvious reason;
- People of color were between 1½ and 2½ times more likely to be targeted than one would expect from their presence in the population; and
- 15% of operator initiated surveillance on women was for voyeuristic reasons.

Mitigation of Equal Protection Risks

Many PTA cameras are not controlled by operators in real time. For instance, operators cannot control the direction, pan, tilt, or zoom of cameras installed in buses and trains. Diversity training to increase operator's cultural awareness and supervising operators' camera usage can address risks of discriminatory surveillance practices. Significantly, RTP's proposal to share PTA live feeds does not include giving law enforcement agencies the ability to control the direction or focus of the cameras.

D. Identification of Individuals

Identification is the act of connecting data to particular individuals.[12] Much of the anxiety surrounding public video surveillance is premised on concerns that government agencies are identifying each person who comes into view of surveillance cameras and keeping a history of their whereabouts.

Surveillance cameras in public spaces can chill speech and association by preventing people from remaining anonymous. For instance, a government camera recording the entrance to a building where an organization holds meetings could reveal associations as readily as a membership list.

Anonymity is important because it (i) enables people to more freely vote, speak, and associate by protecting them from the danger of reprisal,[13] and (ii) provides a means for an unpopular writer to ensure that readers will not pre-judge her message simply because they do not like its proponent.[14] The Supreme Court has upheld the importance of anonymity by:

---

[11] Clive Norris & Gary Armstrong, CCTV and the Social Structuring of Surveillance, Crime Prevention Studies, Vol. 10, at 157-178 (1999); Michael J. Dee, The Use Of CCTV To Police Public Spaces : A Case Of Big Brother Or Big Friend?, at 12-13 (Vienna, Austria, 2000).
[12] Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 511(Jan. 2006).
[13] A Taxonomy of Privacy, 154 U. Pa. L. Rev. at 515.
[14] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995).

- Striking down statutes requiring petition circulators to wear identification badges because identification discouraged participation in the circulation process;[15]
- Striking down statutes prohibiting the distribution of anonymous campaign literature and noting "a respected tradition of anonymity in the advocacy of political causes";[16] and
- Preventing a state from compelling the NAACP to disclose its membership lists.[17]

Surveillance conducted by PTAs also raises identification risks because it is conducted as a condition of using public transportation services. Few rights guaranteed by the First Amendment can be enjoyed without moving about. To associate with others in political activities or pursue religious beliefs, one must travel to the place where their associations meet. If the modes of travel are monitored and individuals' identities are ascertained and recorded, it could be possible to correlate who travels with whom. Sharing PTA live feeds with law enforcement agencies heightens these concerns.

Mitigation of Identification Risks

PTAs have not implemented surveillance system for the purpose of identifying each member of the traveling public. The public's risk of being identified from PTA surveillance footage shared with law enforcement is no different than in any ordinary investigation. Identification risks can further be reduced by implementing policies that prohibit law enforcement officials from using live feeds or archived footage to identify individuals except as necessary for a lawful investigation.

E. Aggregation of Video Surveillance Data

Aggregation is the gathering together of various pieces of information from multiple sources about a person.[18] There is a significant difference between public information that is difficult to obtain from multiple locations, and a computerized summary of that information located in a single clearinghouse.[19]

Aggregation upsets an individual's expectations about how much information they actually reveal to others by consenting to disclose certain information.[20] Data subjects may believe they are only sharing one piece of information, however, if that information is combined with other types of information, it can begin to form a portrait of the person.[21] Aggregation can also create interpretation problems where the data compilation used to make a decision about someone is

---

[15] Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 199-201 (1999).
[16] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343 (1995).
[17] Nat'l Ass'n for Advancement of Colored People v. State of Ala. ex rel. Patterson, 357 U.S. 449, 462-6 (1958) See also, Brown v. Socialist Workers' 74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations").
[18] Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 507 (Jan. 2006).
[19] See U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 764 (1989).
[20] A Taxonomy of Privacy, 154 U. Pa. L. Rev. at 508.
[21] A Taxonomy of Privacy, 154 U. Pa. L. Rev. at 507.

incomplete or results in a distorted portrait of the person because the information is incomplete or disconnected from the original context in which it was gathered.[22]

Mitigation of Aggregation Risks

PTAs typically store and retrieve video footage by location, date, time, and camera identifier; the footage is not connected to any personal identifier. Accordingly, the footage cannot be automatically linked with any other personally identifiable data sets. Law enforcement agencies accessing PTA live feeds and archived footage should only attempt to identify individuals appearing on PTA footage on a case-by-case basis as part of a lawful investigation.

F. Potential Misuses of Video Surveillance Data

Misuses of public video surveillance systems can occur at the collection stage. For instance, officers have faced discipline for focusing cameras on women's breasts and buttocks in Tuscaloosa,[23] San Francisco,[24] and Worcester, England.[25]

Another potential misuse is the improper disclosure of surveillance data by authorized users. The disclosure of a person's location could, for example, heighten that person's vulnerability to property theft or physical harm. The damage caused by improper disclosures is not simply that the data has been disclosed, but that the promise made to keep the information confidential has been broken.[26] Examples of improper disclosures of surveillance footage that have already occurred include:

- Using police databases and surveillance footage to blackmail married patrons of gay establishments;[27] and
- Posting government surveillance footage of a young man committing suicide in a public area to a public website.[28]

Mitigation of Potential Misuses

PTAs control the collection of the surveillance footage; therefore, the potential sharing of live feeds with law enforcement agencies will not increase the risks of misuse at the collection stage. With regard to risks of improper disclosures, the disclosure of confidential information obtained in criminal investigations is unlawful.[29] Law enforcement agencies wishing to participate in a program involving the sharing of PTA live feeds should adopt policies that: (i) set forth the appropriate access and dissemination of PTA footage; (ii) prohibit inappropriate dissemination of

---

[22] A Taxonomy of Privacy, 154 U. Pa. L. Rev. at 508-511.
[23] Jon Gargis, Strip Traffic Camera Follows Pedestrians Home, The Crimson White (Sept. 15, 2003).
[24] SF Cop Accused Of Ogling Women On Duty, SFGate (Apr. 20, 2005).
[25] Andrew Parker, Perveillance of CCTV Operator, The Sun (Feb. 14, 2007).
[26] A Taxonomy of Privacy, 154 U. Pa. L. Rev. at 527.
[27] Toni Locy and Avis Thomas-Lester, Lieutenant Allegedly Acted Alone, Washington Post, p. C01 (Nov. 27, 1997).
[28] Murray Weiss, Bx. Cop Caught in 'Net-Suicide-Video Scandal, New York Post (Jun. 22, 2004).
[29] Cal. Penal Code §146g.

footage; and (iii) punish individuals who inappropriately disclose footage. Participating agencies should also conduct audits and monitor system operations to prevent and identify instances of misuse.

4

Part 4. Collection of Surveillance Data

A. Authorization

Agencies do not need an explicit statutory provision to employ methods of observation commonly available to the public at large.[30] Nevertheless, video surveillance systems operated by PTAs have roots in federal law. For instance, the Federal Transit Administration (FTA) requires agencies receiving urbanized area grant program funds to spend 1% of the grant award on security improvements, including increased camera surveillance.[31] Similarly, United States Department of Transportation regulations outline contents of security plans for certain rail systems.[32] Moreover, video surveillance systems received considerable attention in the Transit Security Design Considerations developed by the FTA to aid transit agencies in developing security strategies.[33]

B. Camera Deployment

PTA video surveillance cameras record PTA employees and the public in monitored areas. PTAs are responsible for the placement of cameras and decisions about where to install cameras are influenced by each PTA's goals and available funding. Generally, PTAs operate cameras at:

- Stations (including elevators),
- Platforms,
- Bus shelters and terminals,
- Passenger parking areas,
- Onboard vehicles (including passenger and operator areas),
- Storage yards,
- Administrative areas,
- Rights of way and track switches
- Rail crossings, and
- Tunnels and portal entrances.

C. Information Potentially Collected By PTA Surveillance Cameras

Certain PTA cameras capable of panning, tilting, and zooming are programmed with a standard tour that can be overridden by a camera operator. The cameras record images of people and vehicles entering each camera's field of view. Specifically, cameras may capture facial images of passengers and employees as well as members of the public on or near the PTA's property.

---

[30] Dow Chem. Co. v. United States, 476 U.S. 227, 233 (1986).
[31] 49 U.S.C. §5307(c)(1)(j).
[32] 49 C.F.R. Part 659.
[33] U.S. DEPT. OF TRANSP. Fed. Transit Admin., Transit Security Design Considerations – Final Report, (Nov. 2004).

Cameras may also collect textual information, including license plate numbers, street and business names, and writing on people's clothing and belongings.

Digitally recorded footage may be supplemented with "metadata" – information about the recording itself or the subjects recorded in captured images that is used to manage live feeds, store feeds, and increase the usefulness of the footage. For instance, footage may be supplemented with the name and location of the camera that recorded the footage as well as the date and time of the recording. Facial images and the text captured by PTA cameras may be rendered machine-readable through facial recognition or optical character recognition software depending upon the quality of the footage and the PTA's resources.

Generally, PTA video surveillance footage of people traveling in public should be treated as confidential information.[34]

D. Notice of Video Surveillance

Fair Information Practices

In 1973, the United States Department of Health, Education, and Welfare ("HEW") published a groundbreaking report responding to concerns that harmful consequences could result from the storing of information related to individuals in computer systems. That report articulated the following principles HEW deemed essential to the fair collection, use, storage, and dissemination of personal information by electronic information systems:[35]

1. There must be no personal data record keeping systems whose existence is secret;
2. There must be a way for an individual to learn what information about him is in a record and how it is used;
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used for other purposes without his consent;
4. There must be a way for an individual to correct a record of information about him; and
5. Any agency creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

In 1980, the Organization for Economic Cooperation and Development ("OECD") published its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The OECD Guidelines articulated eight Fair Information Practices that incorporated the HEW principles and are universally recognized as a foundation upon which to build privacy legislation and policies.[36] The fair information practices provide rules governing the processing of data subjects' personal

[34] See Cal. Veh. Code § 21455.5(f)(1) (classifying as confidential photograph records made by automated traffic enforcement systems).

[35] U.S. DEPT. OF HEALTH, EDUC., & WELFARE, Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems, at xx-xxi (1973).

[36] NATL. CRIM. J. ASSN., Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems, at 22 (2002).

data.[37] One of the fundamental principles is providing notice of data collection and data management practices to data subjects.

Notifying the Public About the Collection and Sharing of Surveillance Data

PTA cameras are typically visible and alert individuals that they are being monitored. PTAs also post notices where the public is under video surveillance. Moreover, even if the public fails to observe the cameras and the signs, PTAs can publish privacy impact assessments or other notices on their websites.

An initiative involving the sharing of PTA live feeds with law enforcement should assess the extent and types of notice it will provide to the public. Notifying the public that real time PTA video feeds will be shared with law enforcement can:

1. Promote public confidence by increasing the transparency surrounding how PTA video footage is used;
2. Invite constructive comments regarding the operation of the video surveillance system;
3. Hold the law enforcement agencies accountable for safeguarding the footage; and
4. Deter prospective offenders by informing them that their conduct on PTA property could be observed in real-time by law enforcement officials.

Public notice can be provided by any of the following:

- Issuing a press release;
- Posting a statement in a prominent location on the participating agencies' websites;
- Publishing privacy impact assessments and policies governing participating agencies' use of PTA footage;
- Sending written notice to a city's elected leadership; or
- Posting additional signage informing the public that live feeds may be made available to law enforcement agencies.

[37] Barbara Crutchfield George, *et al.*, U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive, 38 Am. Bus. L.J. 735, 752 (2001).

5

Part 5. Access to and Dissemination of Surveillance Data

A. Live Feeds Distinct From Archived Footage

Live feeds are video surveillance footage accessible in real-time.

Archived footage is essentially a database containing video recordings stored for future use and organized by date, time, location, and camera identifier. The amount of archived footage available for inquiries depends upon the number of cameras deployed by the particular PTA and its retention policies.

The real-time monitoring of live feeds by law enforcement officials creates different privacy concerns than access to archived footage. Accordingly, this Report addresses live feeds and archived footage separately.

B. Law Enforcement Access to PTA Surveillance Footage

Law enforcement officials have a duty to investigate crimes and collect various types of information in order to identify potential suspects and witnesses. Access to a PTA's live feeds can:

- Bring crimes, such as assaults taking place on PTA property, to a police officer's attention as they occur;
- Help police officers to track and apprehend suspects fleeing on public transportation; and
- Provide critical information to first responders responding to accidents or criminal acts such as hostage situations or bomb threats.

Archived footage can play an important role in the investigation of crimes and can be utilized to help create investigative leads, identify suspects and witnesses, and prosecute offenders.

C. Law Enforcement Dissemination of PTA Surveillance Footage

Agencies participating in a data sharing initiative involving access to PTA video feeds should develop policies that implement the following discussions.

1. Copying of PTA Footage

PTAs that choose to provide law enforcement agencies access to their live video feeds should consider prohibiting those agencies from recording and retaining the footage. This would confirm the PTA's status as the official repository of the footage captured by its cameras.

PTAs routinely provide copies of certain segments of their archived footage to law enforcement agencies conducting criminal or intelligence investigations. PTAs processing law enforcement requests for footage typically log each instance where footage is provided. Law enforcement agencies receiving PTA footage make that footage part of a case file and it should be maintained and secured in the same manner as other evidence comprising that file.

2. Sharing PTA Footage with Other Law Enforcement Agencies

Law enforcement officials have a duty to investigate crimes. As such, they collect, analyze, disseminate, and retain a variety of information, including copies of surveillance footage, to identify and exhaust investigative leads. This evidence is then shared with prosecutors, who make charging decisions and ultimately present the evidence during a trial.

During the course of a criminal investigation, it may become necessary to share surveillance footage across jurisdictions. For instance, an agency possessing footage may release an image of an armed suspect to other agencies over a law enforcement network. Likewise, a probation officer[38] may request a copy of certain archived footage to monitor or verify the whereabouts of a probationer. There may also be instances where multiple law enforcement agencies investigate the same crime.

Law enforcement agencies should follow their existing policies regarding interagency data sharing when considering the sharing of PTA footage with other law enforcement agencies.

3. Sharing PTA Footage for Audit Purposes

Law enforcement agencies implement policies and procedures to mitigate privacy risks associated with the collection and use of sensitive data about individuals. Audits are conducted to confirm that agencies are adhering to those policies. Such audits may be conducted internally or by a separate public or private entity. Law enforcement agencies may allow auditors to view live feeds and archived footage where it is necessary to complete an audit.

4. Sharing PTA Footage Pursuant to Court Order

(i) A Criminal Defendant's Access is Limited to Formal Discovery

Prosecutors are required to disclose to defendants or their attorneys certain information in the possession of investigating agencies including relevant surveillance footage.[39] Criminal defendants may access PTA surveillance footage through the formal discovery process or as a member of the general public.

(ii) Responding to Subpoenas for Footage

Law enforcement agencies may receive subpoenas for PTA surveillance footage. For instance, a plaintiff in a divorce proceeding might seek surveillance video of a cheating spouse. Requests for PTA footage that has been incorporated into a case file should be responded to in the same manner as if the subpoena sought copies of other records contained in the agency's case files.

[38] Probation officers are considered law enforcement officials. Cal. Penal Code §830.5.
[39] Cal. Penal Code §1054.1.

5. Limited Sharing of PTA Footage with the Public

There may be instances where law enforcement purposes are furthered by sharing PTA footage with the public. Whether and to what extent PTA footage may be shared with the public depends upon the type of entity receiving the footage and the circumstances surrounding the disclosure.

(i) Archived Footage May Be Shared With the Public in Certain Instances

Sharing PTA surveillance video with the public could exacerbate the privacy risks discussed above and could compromise the security of PTA property and vehicles. For instance, video footage of transit platforms would reveal the position of cameras, the cameras' capabilities, the area captured by the cameras, and the areas where the view of the cameras cannot reach. This information could be used to plan an attack on PTA property and the millions of riders who use public transportation every day.

Nevertheless, images collected by PTA cameras could be useful in line-ups and in identifying suspects, victims, and witnesses of crimes on or near PTA property and law enforcement agencies may share footage with the public for these purposes. As such, limited disseminations will take place during the course of an investigation. For instance, an officer may show an image taken from PTA surveillance footage to a potential witness and ask if they recognize the person in the image.

Surveillance images may also be useful in enlisting public aid in seeking missing persons or in apprehending suspects. In these instances, participating law enforcement agencies may release to the public or news media footage collected by a PTA that reasonably identifies missing persons, criminal suspects, or individuals who pose a threat of substantial harm to the public.

(ii) Responding to Public Records Requests

Law enforcement agencies may receive requests for PTA footage pursuant to the California Public Records Act. Law enforcement agencies should respond to such requests in the same manner as if the requestor sought copies of other records contained in the agency's case files.

6

Part 6. Law Enforcement Retention of PTA Footage

A. How Retention Periods Influence Privacy Risks

Justice practitioners and policy-makers are reluctant to destroy records because seemingly irrelevant or untimely information may acquire new significance as an investigation evolves and new details emerge.[40] Deleting surveillance footage could impede investigations and result in fewer cases being solved.

Nevertheless, the indefinite retention of surveillance data makes a vast amount of information about law-abiding citizens available for potential misuse, accidental release, or unauthorized disclosure. Additionally, storing video surveillance footage for long periods of time can be viewed as a form of undesirable social control.

Establishing retention guidelines that take into consideration the purposes for which the surveillance footage was collected as well as the sensitivity of the footage helps to mitigate the public's privacy concerns, but can also reduce the agency's costs of storing the numerous back-up media necessary to recover from an unforeseen disaster.

B. PTAs' Retention of Video Surveillance Data

PTAs' retention policies and the number of cameras they deploy influence how much archived footage is available for law enforcement inquiries. Many PTAs index, store, and maintain video footage for a fixed period of time,[41] after which the files are automatically recorded over unless they were previously identified for longer retention. PTAs typically retain certain segments of video footage for a longer period of time where the footage:

- Captures an occurrence that may subject the PTA to civil liability;
- Contains evidence of criminal or suspicious activity;
- Has value for training purposes; or
- Was requested by or provided to another agency.

C. Law Enforcement's Retention of PTA Footage

Law enforcement agencies should retain PTA footage in accordance with the agency's retention policies.

---

[40] See 68 Fed. Reg. 14140 (2003).

[41] California law anticipates the retention of transit video footage for at least one year. See Cal. Gov. Code §§53160; 26202.6; and 34090.6l. See also Ca. Atty. Gen. Op. 02-207 (Dec. 20, 2002). New transit security systems must be capable of storing one-year's worth of video with certain limited exceptions. See Cal. Gov. Code §§53162; 26206.8; 34090.8; and Cal. Pub. Util. Code §99164.

7

Part 7. Quality of Surveillance Data

A. Data Quality, Conceptually

The quality of a particular set of information can be expressed as the extent to which the data is:

- Available or readily retrievable;
- Appropriate for the specific task;
- Regarded as true and correct;
- Easy to interpret; or
- Unbiased and impartial.

Agencies can use these attributes to describe the accuracy and reliability of the data they use to make decisions. The ability to describe why data is reliable inspires trust in the justice system and the agencies that use the information.

B. Quality of PTA Surveillance Footage

The primary data quality issue regarding video surveillance footage is poor image resolution. Poor lighting and low contrast due to overexposure, reflection, adverse weather conditions, or shadows can result in a poor image capture. Other times, the subject may be too far away for the capabilities of the camera to capture. Motion blur can also result in an unclear image. Hats, scarves, and sunglasses might obscure all or portions of an individual's face and limit the usefulness of the footage.

Another aspect of data quality is influenced by the interaction between the camera operator and the surveillance system. If the user is overwhelmed by information or processes displayed by the system, or if he does not possess the local knowledge of the surveillance area to understand where the events he is seeing are taking place, he will not be able to absorb accurately the data presented to him and perform his tasks such as selecting which camera feeds to record or identifying where to request law enforcement resources.

C. Integrity of Archived Footage

PTAs generally store video footage in a manner that does not permit additions, changes, or deletions to the recorded images. Likewise, PTA storage media are usually permanent, reliable, and backed-up to ensure availability after a disaster.

D. No Individual Right to Access or Challenge PTA Surveillance Data

PTAs do not routinely index or retrieve footage by a personal identifier, therefore there is no method by which to extend to individuals a right to access or challenge surveillance footage. Moreover, PTA surveillance systems simply collect scenes captured by cameras; such footage

cannot be changed and is typically presumed to be accurate.[42] There is also less of a need to provide individuals with an opportunity to access PTA surveillance data where the footage is not generally released to the public.

[42] A printed representation of images from a video is presumed to be an accurate representation of the images it purports to represent. Cal. Evid. Code §1553.

8

Part 8. Accountability Safeguards

Many privacy concerns can be mitigated by holding law enforcement agencies accountable for the information they collect and how they subsequently use that information.

A. Audit Logs

Audit logs deter and uncover authorized users' abuse of a data system. Law enforcement officers may be discouraged from inappropriately copying and disclosing surveillance footage if they know that their access to that data is being monitored and recorded.

Law enforcement agencies that receive copies of archived footage from PTAs already log the footage as evidence and track its chain of custody. Audit trails should be built into any systems that make PTA live feeds available to law enforcement agencies. These trails should permit supervisors to identify which officers viewed what footage at what time.

B. Secondary Dissemination Logs

PTA surveillance footage should be considered for official use only. Since it is collected by a PTA and is shared with law enforcement agencies for specified purposes, any subsequent dissemination of the footage by the law enforcement agency should be recorded in a log that contains:

1. A description of the footage disseminated, including the date, time, and location of the recorded footage and the case number containing the footage;
2. The name of the person copying/transmitting the footage;
3. The date and time the footage was released;
4. The identity of the individual to whom the footage was released, including their agency and contact information; and
5. The purpose for which the footage will subsequently be used.

C. Monitoring and Conducting Audits

Audits help to ensure that law enforcement agencies are following the policies developed to regulate the collection, use, and dissemination of PTA surveillance footage. Auditors should review a participating law enforcement agency's operations, audit logs, and case files to determine if the agency is appropriately accessing and utilizing the PTA live feeds and archived footage. A written report of findings should be prepared.

D. Policy Awareness and Training

Law enforcement officials with access to PTA live feeds and archived footage should be trained regarding:

1. The technical aspects of the system;
2. The privacy risks discussed in this assessment;
3. Limits on the access, use, and dissemination of PTA surveillance footage;

4. How these limits protect the public;
5. Penalties for violating the policies; and
6. Disciplinary procedures if the policies are violated.

Employees should be able to easily access the policies and any interpretive guidelines. Policy education and awareness surrounding the use video surveillance data systems is a continual process that should be revisited and updated as laws and regulations evolve over time. Each participating law enforcement agency should ensure that its employees have completed the necessary training.

9

Part 9. Security Safeguards

Ensuring that PTA live feeds remain secure is a necessary step to addressing the public's privacy concerns. Live feeds shared with law enforcement agencies should be transmitted via a secure network that complies with the Federal Bureau of Investigations Criminal Justice Information Services network security standards. Participating law enforcement agencies should also implement physical and technical safeguards to prevent unauthorized access, use, and disclosure of PTA live feeds.

500 North Dearborn Street, Second Floor
Chicago, IL 60654
312.755.5700 p 312.755.5720 f
krasnowsaunders.com

About the Authors

Krasnow Saunders Kaplan & Beninati LLP provides pragmatic, creative, and imaginative solutions to the legal challenges facing businesses and their owners. We are straight-talking business lawyers who represent a broad range of clients in diverse industries and geographic regions across the country, including publicly-held corporations, large financial institutions, family owned businesses, and entrepreneurs. We view our job as helping clients evaluate the risks and benefits of alternative courses of action and the likelihood of the risks occurring.

As privacy counselors, we distinguish ourselves by helping you assess how privacy fits into your particular business environment. We understand that privacy issues are influenced by many of the same principles of trust that facilitate effective social and business relationships. We offer comprehensive counseling on privacy and data security issues to help clients proactively implement data protection safeguards as well as respond to privacy incidents, which may trigger notification requirements, exposure to litigation, and investigation by regulatory agencies. Our multi-disciplinary capabilities allow us to assist clients with internal investigations, regulatory enforcement actions, and civil litigation.

Our attorneys are certified by the International Association of Privacy Professionals and have been on the forefront of advising clients on the benefits and risks of newly emerging data collection and sharing technologies. Our privacy and data security focus areas include:

- Providing regulatory and compliance advice on the collection, use, protection, sharing and retention of data across a broad range of industries.
- Preparing privacy impact assessments of newly emerging technologies and data sharing initiatives.
- Auditing existing security and data sharing policies to assess weaknesses.
- Developing policies, practices, and procedures that reduce privacy risks and exposure to data breaches.
- Responding to data breach incidents.
- Designing transactions to protect informational assets and conducting data security and privacy due diligence.
- Assisting in litigation that may arise as a result of a data breach or violation of privacy law.