KRASNOW SAUNDERS KAPLAN & BENINATI LLP

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

AGENCY-WIDE SANDAG PRIVACY IMPACT ASSESSMENT

April 12, 2017
(updated by SANDAG staff June 2018)

Prepared for

SANDAG

1

Why and How this Report was Prepared

SANDAG takes its role in protecting individual privacy while serving the public very seriously. One way to assure the public that SANDAG is appropriately balancing these sometimes competing goals is by communicating the types of information SANDAG collects and how it uses and safeguards that information. SANDAG believes that being transparent about the data it collects (a) gives members of the public coming into contact with SANDAG programs and services more control and confidence that their information will be appropriately handled and (b) helps the public make informed decisions.

To prepare this report, SANDAG conducted a data inventory to document the scope of data it collects, where it is being held, with whom it is being shared, and how it is being transferred. SANDAG also created the framework of this report to best present the public with insights into SANDAG privacy practices by synthesizing the organization and themes discussed in:

- Privacy impact assessments published by federal agencies[1];
- The Fair Information Practice Principles of many governmental organizations such as the U.S. Federal Trade Commission, the Organization for Economic Cooperation and Development, and the White House's National Strategy for Trusted Identities in Cyberspace; and
- The Federal Trade Commission's (FTC) principals for organizations implementing consumer privacy programs.[2]

Ultimately, this report is meant to provide the public with a view of how SANDAG incorporates privacy and security protections – from start to finish – into its processes when handling Personally Identifiable Information (PII)[3] and other types of confidential information and, by doing so, demonstrate that the SANDAG collection, use, and maintenance of personally identifiable and confidential information meets applicable legal standards and does not unduly interfere with personal privacy interests. SANDAG believes that this report provides useful information and welcomes comments on how it can improve its practices.

---

[1] Section 208 of the E-Government Act of 2002, 107 Public Law 347, 116 Stat. 2899 requires agencies to conduct privacy impact assessments (PIAs); See also PIAs developed by the U.S. Department of Justice, U.S. Department of Homeland Security, U.S. Department of Transportation, and the U.S. Census Bureau.

[2] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012).

[3] PII is information about an individual that distinguishes or traces an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; or is linked or linkable to an individual, such as medical, educational, financial, and employment history.

2

The SANDAG Mission Requires it to Collect Information

SANDAG engages in regional cooperative comprehensive planning, programming, and implementation of infrastructure projects, and assists its member agencies, which include the 18 cities and county government within the San Diego region.

SANDAG responsibilities require it to obtain information so that it can provide programs and services such as:

- Coordinating with other San Diego agencies to create strategies that balance the existing and anticipated population, housing, and employment growth with habitat preservation, agriculture, and infrastructure needs;
- Identifying trends and preparing estimates and forecasts of the region's population, jobs, and housing to inform long-range plans and to inform and serve the public;
- Identifying the level of infrastructure investment required to ensure mobility choices by connecting transportation networks to homes, schools, work, shopping, and other activities;
- Working to preserve open space and efficiently use energy and transportation resources;
- Operating commuter programs such as carpool, vanpool, 511 travel information, and the Freeway Service Patrol, and collecting data so that these programs better inform and serve the public;
- Operating the South Bay Expressway – State Route 125 (SR 125) and Interstate 15 Express Lanes toll facilities and planning for a managed lanes network;
- Monitoring and reporting on transportation system performance and sharing this information to improve operations, and to inform and serve the public;
- Improving the network of transit services and constructing an active transportation network of bicycle and pedestrian paths;
- Promoting regional collaboration in the acquisition and maintenance of public safety data and technology; and
- Operating the Automated Regional Justice Information System (ARJIS)

SANDAG accomplishes these tasks by gathering a data-driven understanding of the San Diego region's infrastructure systems, how and when they are used, how changes can be made with minimal adverse impact on users, and the likely results of its proposed changes. As discussed more fully below, SANDAG designed its processes for collecting this data with attention to the public's legitimate privacy concerns.

3

Ways SANDAG Reduces Privacy Risks Generally

Generally, a government agency's collection of information about particular individuals raises privacy concerns, but those concerns can be difficult to articulate. This portion of the report provides an overview of the types of privacy concerns that could be raised related to the data that SANDAG collects and maintains and the efforts it makes to minimize those concerns.

A: SURVEILLANCE

1: RECORDING WHERE AND WHEN PEOPLE TRAVEL CAN CREATE CHILLING EFFECTS

People may consider the collection of information about their whereabouts as a form of surveillance. At its simplest, surveillance occurs when organizations pay close attention, in routine and systematic ways, to specific individuals. The potential harm of surveillance comes from its use as a tool of social control. The mere possibility of surveillance has the potential to make people feel uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition.[4] These potential consequences are referred to as "chilling effects."

2: MITIGATION STRATEGIES

SANDAG observes and collects information such as travel behavior data, but does not conduct surveillance on specific individuals. SANDAG mitigates any potential chilling effects related to its data collection efforts by:

- Notifying the public about what personally identifiable information (PII) it collects and how it is used before collecting the data;
- Seeking, where practicable, individuals' consent for the collection and use of their PII;
- Providing individuals an opportunity to opt out of having their PII collected;
- Limiting the amount of data collected to that which is reasonably necessary to accomplish the specified purpose;
- Limiting how long the PII is retained;
- Using the PII only for purposes compatible with the reasons for which it was initially collected; and
- Holding itself and its employees accountable for complying with SANDAG privacy policies and practices.

[4] Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 493 (2006).

B: IDENTIFICATION

1: IDENTIFICATION MAKES IT EASY TO CONNECT SEPARATE PIECES OF DATA

Identification is the act of connecting data to particular individuals.[5] Identification is related to (a) the disclosure of information (i.e., something about the person's identity) and (b) the consolidation of other pieces of information with the identity of a person,[6] both of which are discussed below. The potential harms of identification stem from the ability to connect PII (e.g., name, fingerprint) to a stream of collected data. Specifically, identification can:

- Make people vulnerable by allowing the connection of information that can be used to bypass password recovery mechanisms for online accounts[7];
- Enable surveillance by facilitating the monitoring of a person;
- Increase the chilling effects discussed above; and
- Inhibit one's ability to be anonymous.

2: MITIGATION STRATEGY

SANDAG does collect data which, if left in its raw form, could be used to connect separate pieces of information to a particular individual. SANDAG mitigates identification risks by, where practicable, "scrubbing[8]" the data (a) at the time of collection, (b) before the data is used, or (c) before the data is disseminated internally or externally. In some cases, other agencies share PII with SANDAG. When this occurs, SANDAG has measures in place to protect the confidentiality of the data so that it is not shared, disseminated, or transferred.

C: SECONDARY USE

1: PEOPLE CANNOT ALWAYS ANTICIPATE HOW DATA MAY BE USED IN THE FUTURE

Secondary use occurs when data is subsequently utilized, without the data subject's consent, to accomplish a goal that is unrelated to the original purpose for collecting the data. Examples are datasets that are collected for specific research or statistical purposes, but then re-used to answer other research questions that were not disclosed to the data subject.

The potential harm of secondary use is that it undermines people's reasonable expectations as to how the PII about them will be used in the future or who will use the information. Another potential source of harm surrounding secondary use

---

[5] Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. at 510.

[6] Not all consolidation involves identifying information.

[7] See Kim Zetter, Palin E-Mail Hacker Says It Was Easy, Wired.com (Sept.18, 2008) (describing how a hacker used Google searches to obtain the answers to Sarah Palin's security questions on her email account, specifically her birthdate, zip code and where she met her spouse).

[8] See Appendix A for additional information about how data can be scrubbed of identifying fields.

is that the data may be misunderstood when it is removed from its original context and that the misunderstanding may have real-world repercussions.

2: MITIGATION STRATEGY

In most cases when SANDAG collects PII from individuals, it discloses that the data could be used for a broad range of research or planning purposes. Collecting new data can pose a heavy time or cost burden on the public and there are legitimate reasons SANDAG might use data for purposes unrelated to its original collection. For instance, data collected for one purpose might be analyzed again to:

- Avoid costs and burdens on data subjects of collecting the same information multiple times;
- Corroborate or challenge conclusions of the original project; or
- Apply new tests or hypotheses that were not available at the time the data was originally collected.

SANDAG mitigates risks raised by the secondary use of PII by limiting secondary use to instances where (a) it is not possible or practicable to seek consent from the data subjects, (b) the PII is essential to the research or project, (c) using the PII is not likely to adversely affect the data subjects, and (d) it protects the data subjects' privacy and safeguards the PII. Furthermore, SANDAG prohibits others from selling or reusing data in its contracts.

D: CONSOLIDATION

1: COMPILING VARIOUS PIECES OF INFORMATION ABOUT A PERSON CAN REVEAL THE PERSON'S PERSONALITY

Consolidation is the gathering together of pieces of information about a person.[9] People give out bits of information every day in different settings, only revealing a small part of themselves in each context, and they expect that each disclosure reveals relatively little about their personality. When these pieces are compiled together, however, that information paints a portrait of that individual's personality that can include his or her political, social, educational, cultural, economic, philosophical, or religious beliefs.[10]

The potential harms of consolidation are that it may:

- Enhance the harms generated by secondary use;

[9] Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. at 506. Solove uses the term "Aggregation." This report uses the term "consolidation" to avoid confusion with the phrase "aggregate data", which refers to scrubbed statistical summary information about groups of persons.

[10] See Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. at 507.

- Unsettle individuals' expectations regarding how much information they actually reveal to others; and
- Create interpretation problems wherein the particular data compilation is incomplete or results in a distorted portrait of the person (because the information is disconnected from the original context in which it was gathered).

2: MITIGATION STRATEGY

SANDAG collects small pieces of information about people that could potentially be consolidated into more revealing information. SANDAG remediates consolidation concerns by:

- Being transparent about what PII it collects and how and why it may be combined;
- Seeking, where practicable, consent from data subjects prior to consolidating PII about them;
- Providing, when practicable, individuals an opportunity to opt out of having their PII consolidated;
- Only consolidating PII where it is essential to fulfill an agency mission;
- Limiting the amount of PII consolidated to that which is reasonably necessary to accomplish the specified purpose;
- Limiting the consolidation of PII to instances where it will not adversely affect the data subject; and
- Holding itself and its employees accountable for complying with SANDAG privacy policies and practices.

E: BREACH OF CONFIDENCE

1: BREACHING CONFIDENTIALITY CAN DAMAGE THE PUBLIC'S TRUST

A breach of confidence is a broken promise to keep a person's information confidential. The potential harm caused by a breach is not simply that information has been disclosed, but that the promise made to the data subject has been broken. Protections against breach of confidentiality help promote certain relationships that depend upon trust, such as the relationship between the public and their government.

2: MITIGATION STRATEGY

SANDAG mitigates risks of data breaches and misuse of PII by:

ADMINISTRATIVE SAFEGUARDS	▪ Analyzing and managing potential data security risks; ▪ Monitoring data system and network activity; ▪ Identifying which employees and vendors need to access PII to perform their duties; ▪ Limiting employees' and vendors' access to PII to the minimum amount necessary to perform their duties; ▪ Implementing procedures for granting, supervising, and terminating employees' and vendors' access to PII; ▪ Continuing to develop policies and training employees and vendors about how to safeguard PII; ▪ Developing procedures for investigating and resolving security vulnerabilities and incidents; ▪ Requesting that employees and vendors report potential security incidents to SANDAG supervisors; ▪ Setting standards for creating, changing, and safeguarding passwords; ▪ Developing and testing contingency plans; ▪ Including provisions in contracts with third parties to ensure they appropriately safeguard PII;
PHYSICAL SAFEGUARDS	▪ Limiting physical access to electronic data systems (e.g., server rooms and telephone equipment closets); ▪ Requiring visitors to sign in prior to entering SANDAG offices; ▪ Installing cameras in public areas of SANDAG offices; ▪ Developing and implementing facility security plans; ▪ Requiring staff to use data security features on equipment used for SANDAG purposes; ▪ Requiring that research records containing PII or confidential information be marked and placed in a secure location; ▪ Documenting security repairs and modifications; ▪ Implementing procedures governing the destruction or removal of servers containing PII; ▪ Selecting appropriate methods to dispose of PII and the servers on which it is stored; ▪ Having disaster recovery plans and systems in place;

TECHNICAL SAFEGUARDS

- Implementing role-based access controls that limit access to PII to the minimum amount necessary to perform that role's function;
- Centrally managing and assigning unique user IDs for tracking that user's activity;
- Imposing appropriate requirements for password strength and periodic rotation of passwords;
- Recommend storing passwords in a secure manner;
- Automatically terminating an electronic session (i.e., logging off) after a predetermined time of inactivity;
- Limiting invalid log-in attempts;
- Utilizing encryption systems to protect sensitive information from being accessed or viewed by unauthorized users;
- Building audit controls into information systems that record user activity;
- Protecting PII from improper alteration or destruction;
- Confirming that users are who they claim to be before allowing access to PII;
- Transmitting PII in a manner that prevents unauthorized access to the information; and
- Applying patches to operating systems, firewalls, and anti-virus software.

F: DISCLOSURE

1: RELEASING INFORMATION IMPACTS PEOPLE'S LIVES

Disclosure occurs when information about a person is revealed that impacts the way others judge his or her character. The potential harm of disclosure involves damage to an individual's reputation caused by the dissemination. The risks raised by disclosure are similar to those raised by breach of confidence in that the same data is revealed in both scenarios. Disclosure carries with it the potential chilling effects associated with surveillance. Disclosure also is related to identification as the released information can be traced back to the data subject.

2: MITIGATION STRATEGY

SANDAG mitigates disclosure risks by utilizing the mitigation strategies discussed above for risks associated with surveillance, identification, and breaches of confidence.

4

Location and Travel Pattern Information

A: WHY SANDAG COLLECTS LOCATION AND TRAVEL PATTERN DATA

SANDAG scrubs and aggregates various types of PII to compile statistics useful for monitoring how efficiently the regional transportation system works to develop new transportation strategies. Types of data may include:

- Annual transit ridership;
- Mode share (single-occupancy vehicles, carpool, transit, walking, biking, etc.);
- Travel times and volumes for automobile and transit corridors;
- Annual hours of traffic delay per traveler;
- Housing information in Smart Growth Opportunity Areas;
- Intra-regional traffic volumes into San Diego from surrounding counties; and
- Border wait times for personal trips and goods movement.

SANDAG also collects PII to operate toll road facilities and implement Transportation Demand Management (TDM) programs.

1: ELECTRONIC TOLL COLLECTION OPERATIONS

Streets and Highways Code 31490 authorizes SANDAG to collect tolls electronically. The law protects the privacy of people who use toll roads by limiting who has access to data about where and when they travel. The statute:

- Prohibits (with limited exceptions) SANDAG from selling or disseminating PII about subscribers;
- Requires SANDAG to establish privacy policies and provide those policies to subscribers;
- Requires police officials to have a warrant or certify that exigent circumstances exist before SANDAG can release PII to them; and
- Limits how long SANDAG can retain account-related information.

On State Route 125 South Bay Expressway (SR 125), and the Interstate 15 (I-15) Express Lanes, SANDAG uses Electronic Toll Collection (ETC) to collects tolls. ETC eliminates travel delays associated with toll collection and relies upon Automatic Vehicle Identification (AVI) technologies. AVI works through the use of cameras, radio antennas, toll transponders, and license plates. The AVI matches camera

images and transponder data to process and post transactions to a vehicle owner's *FasTrak*® account.

On SR 125, the ETC system takes photos of all vehicles that travel the facility, including the front of the vehicle and the rear license plates. In the event a vehicle owner does not have a *FasTrak* account, camera images are used to pursue unpaid amounts due. Video cameras are used to monitor cash collection and credit card transactions that occur when motorists use these alternative payment methods.

On I-15, cameras capture images of all vehicles that pass through toll plazas. In the event the AVI cannot accurately identify the transponder, or if the vehicle operator violates the "HOV Only" rule, camera images of the rear license plate are saved; otherwise, camera data is not stored.

License plate numbers are used to obtain information about the owner from other sources (such as the California Department of Motor Vehicles) to identify the owner and pursue unpaid amounts due.

FASTRAK TRANSPONDERS

Radio frequency identification is used to communicate between the toll system and the vehicle transponder. Each transponder transmits a unique identification number. When the ETC system reads a transponder, a date, time, and toll plaza locations are added to the transponder ID and transmitted to the Operations Center, where it is connected to a subscriber's account information (e.g., name, credit card number, billing address, and vehicle information) to process the transaction for payment.

AUTOMATED LICENSE PLATE READERS (ALPRS)

ALPRs are databases resulting from cameras paired with computer algorithms that convert images of license plates into computer-readable data. On SR 125, SANDAG uses fixed cameras to collect still images of each vehicle passing a toll-collection point, including its rear license plate. On I-15, SANDAG uses fixed cameras to collect still images of vehicles.

The images, along with the date, time, and location where each image was taken, are transmitted to a lane controller where the images are processed through optical character recognition (OCR) technology to "read" the license plate. The resulting trip data and images are transmitted to the operations center through a firewall-protected, private secured network. Once there, staff verifies any images that are not automatically matched by AVI system to determine whether the license plate number is associated with a *FasTrak* account. If a license plate can be matched to an account, the

account is charged; if not, staff accesses vehicle registration information to identify the vehicle's owner and pursue the unpaid amount due.

Still image data can include:

- License plate numbers;
- Images of the vehicle including its license plates, make, model, distinguishing features (e.g., bumper stickers, damage);
- State of registration;
- Camera identification;
- Location information (e.g., toll plaza ID); and
- Date and time of observation.

VIDEO FOOTAGE

The SR 125 facility security system uses video cameras to monitor the toll collection facilities, including the in-lane, automated cash and credit card equipment, the ramp buildings, and the Customer Service Center. The footage, along with the date, time, and location where the video was taken, is transmitted to SANDAG digital storage system through a firewall protected, private secured network. Video data is retained for 90 days and is used to verify transaction disputes raised by a customer.

This video data can include:

- License plate numbers;
- Images of the vehicle including its license plates, make, model, distinguishing features (e.g., bumper stickers, damage);
- Camera identification;
- Location information (e.g., toll plaza ID);
- Date and time of observation;
- Images of walk-in customers at the Customer Service Center; and
- Audio recordings.[11]

SR 125 also operates a closed-circuit video camera system as part of the freeway traffic and incident management system, which uses pole-mounted, roadside cameras to monitor the freeway facility, including the lanes, shoulders and median. The video data is transmitted through a firewall-protected, private, secured network for live viewing only to the

[11] If threatened, SANDAG staff in customer-facing roles can press a "panic button" that begins recording audio along with the video.

SANDAG operations center. The data is used by SANDAG and Caltrans to monitor vehicular traffic and to aid in traffic incident and emergency response. The data from this system is not recorded and is not stored.

2: TRANSPORTATION DEMAND MANAGEMENT AND TRANSPORTATION SYSTEMS MANAGEMENT

Sections 132350.1(d) and 132354 of the California Public Utilities Code authorize SANDAG to collect data to help it improve mobility in the San Diego region. Transportation Demand Management (TDM) programs such as the iCommute Ridesharing Program; and Transportation Systems Management (TSM) programs such as Intelligent Transportation Systems, and the Freeway Service Patrol, collect PII from people who use these services. The goal of the TDM and TSM programs is to reduce traffic congestion by encouraging the use of transportation alternatives and by effectively managing the transportation system, both of which in turn reduce environmental pollutants that would otherwise result from commuters driving alone each day. These programs use scrubbed data such as vehicle speeds, locations, and fuel consumption to reduce:

- Emissions;
- Unnecessary trips;
- Vehicle idling;
- Unnecessary accelerations and decelerations; and
- Accidents.

iCOMMUTE RIDESHARING PROGRAM

SANDAG operates the iCommute program to help commuters carpool, vanpool, take transit, bike, walk, and telework. Commuters who participate in the program create an account by submitting their name, contact information, and home and work addresses. After an account is created, commuters can complete a public profile, which is used to match the commuter with other people traveling in the same direction. Public profile information can (but does not have to) include the commuter's:

- Gender;
- Employer;
- Work schedule;
- Usual mode of transportation; and
- Preferences (such as traveling with smokers and people of certain genders, or whether the commuter prefers to be a driver or passenger).

Commuters also can use the website to calculate the cost of their commute and the potential savings associated with trying an alternative mode of transportation. The website also logs each commuter's trip to track their financial and environmental savings.

INTELLIGENT TRANSPORTATION SYSTEMS

SANDAG collects and uses Intelligent Transportation Systems (ITS) data to (a) assess how well the region's transportation systems are performing; (b) manage and respond to traffic incidents and roadside emergencies; (c) identify opportunities for improving the systems; and (d) calculate the impact of proposed infrastructure improvements to inform decision-makers of the best options.

FREEWAY SERVICES PATROL AND THE CALL BOX MOTORIST AID PROGRAM

SANDAG provides assistance to stranded motorists to further its mission of improving the efficiency of the transportation network. Freeway Service Patrol (FSP) drivers help stranded motorists by providing a gallon of gas, jump-starting their vehicles, refilling radiator water, and changing flat tires. The FSP program works in conjunction with the Call Box Program, which connects travelers who experience vehicle problems while on the highway to a 24/7 call center. SANDAG collects personal information about consumers to monitor the number of motorists served by these programs and the specific services performed by FSP and call center staff.

SURVEYS

SANDAG surveys the public to make informed decisions about how to best meet the region's future transportation needs. Surveys, which may be conducted by telephone, by mail, by personal interviews, and through focus groups, can cover a broad range of topics such as (a) when and where people travel; (b) whether they drive alone, carpool or vanpool, walk, bike, or use public transit; and (c) how much their travel activity costs. This information helps SANDAG understand how the region's transportation system copes with growth, development, and other changes.

B: PRIVACY ISSUES RELATED TO LOCATION AND TRAVEL PATTERN DATA

In addition to the general categories of privacy risks described above in Part 3, the following specific risks may be created by the collection, use, and dissemination of location and travel pattern data. Location and travel pattern data can make individuals vulnerable to physical and economic harm. It can disclose the times and places he or she will likely be in the future. Having the data makes it easier for

someone to stalk a person, find their property, or make a social engineering attack (for example, a phishing scam) more credible. Accordingly, California law protects the public's location information by prohibiting the disclosure of a person's home address in certain circumstances, such as when it is collected from a person because he or she is a crime victim, witnessed a crime, registers to vote, is affiliated with a reproductive health services facility, or applies for a state identification card or driver's license.

The Federal Trade Commission considers location information to be sensitive and suggests that entities collecting location and travel pattern data provide "prominent" notice and choices to individuals.[12]

C: HOW SANDAG USES AND DISSEMINATES LOCATION AND TRAVEL PATTERN DATA

1: INTERNAL USES AND ACCESS CONTROLS

Not all SANDAG personnel need the same level of access to location and travel pattern data in order to perform their jobs. Accordingly, SANDAG:

- **Utilizes role-based controls** that limit access to individuals' location and travel pattern data only to those staff that need to know the information to perform their jobs.
- **Implemented approval processes** for determining whether to grant access to personnel outside of the job categories that traditionally need access to location and travel pattern data.
- **Implemented on-boarding and off-boarding procedures** for granting and revoking access to location and travel pattern data for new and departing employees.
- **Minimizes the amount of data** available to personnel to that necessary to perform the job functions.
- **Logs access to data** to detect and investigate suspicious access to location and travel pattern data. SANDAG takes disciplinary action against personnel who inappropriately access location and travel pattern data.

SANDAG uses location and travel pattern data for various purposes, such as to: (a) process enrollments; (b) manage accounts; (c) determine tolls and fees; (d) collect payments; (e) provide subscribers with information about their use of SANDAG services; (f) communicate with subscribers and users;(g) learn how people use SANDAG services; (h) generate aggregated and scrubbed information for statistical analysis; (i) discover and investigate potential violations of SANDAG policies and terms of use; (j) investigate fraud; (k) customize content, services, and

[12] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, 33-4 (2012).

communications; and (l) identify opportunities for improving the transportation system and develop plans for doing so.

2: DISSEMINATION OF THE DATA OUTSIDE OF SANDAG

SANDAG Employee Handbook prohibits personnel from disclosing PII and confidential information, including location and travel pattern data, without authorization and emphasizes that unacceptable use of SANDAG data carries significant penalties up to termination. Additionally, SANDAG does not sell or distribute PII to unrelated third parties for those third parties' marketing purposes without the data subject's express consent.

When it uses a third-party service provider, SANDAG only discloses the minimum amount of location and travel pattern data needed to perform the service. SANDAG contracts with service providers state that SANDAG is the sole and exclusive owner of the personal information and requires providers to:

- Only process PII for purposes specified in the contract;
- Notify SANDAG of any unauthorized access, use, or dissemination of PII;
- Notify SANDAG if they are the subject of a government investigation or proceeding regarding the provider's security or management of PII; and
- Implement reasonable data security safeguards and monitor their systems.

The SANDAG Office of General Counsel responds to law enforcement requests for *FasTrak* transponder or license plate data and only releases that data pursuant to a warrant or where a police official certifies that (a) he is conducting a criminal or traffic collision investigation *and* (b) has good cause to believe that the delay in getting a search warrant would result in (1) danger to an individual's physical safety, (2) flight from prosecution, (3) loss of evidence, (4) intimidation of potential witnesses, (5) serious jeopardy to an investigation, or (6) undue delay of a trial.

Consistent with applicable law, SANDAG may disseminate location and travel pattern data to:

- Transportation and toll agencies for interoperability purposes and to resolve subscriber disputes;
- Contractors that perform services for SANDAG and agree to maintain the confidentiality of the information and use it only as necessary to carry out the duties of their contracts with SANDAG; and
- SANDAG member agencies

iCommute Ridesharing data is used to match drivers and riders for carpooling purposes. The website allows people considered potential matches to contact each other without disseminating their contact information. Drivers and riders using

iCommute agree that certain PII can be shared with other commuters participating in the program.

Personally identifying data elements are scrubbed from TDM data before it is disseminated outside of SANDAG. TDM data is disseminated in reports, planning documents, and proposals for transportation system improvements.

D: HOW LONG SANDAG KEEPS LOCATION AND TRAVEL PATTERN DATA

California law requires that *FasTrak* and ALPR data be deleted after a certain period of time. Specifically, basic account data is deleted 4.5 years after account termination[13] while specific travel data is deleted 4.5 years after payment or resolution of violations.[14]

The retention periods for other types of location and travel pattern data are set forth in SANDAG records retention schedule. SANDAG Records Management Policy requires records containing PII or confidential information to be disposed of (a) promptly upon the expiration of their retention period, and (b) in a manner that does not disclose their content.

E: HOW THE PUBLIC IS MADE AWARE OF SANDAG PRACTICES REGARDING LOCATION AND TRAVEL PATTERN DATA

1: NOTICE OF AND CONSENT TO COLLECTION OF LOCATION AND TRAVEL PATTERN DATA

SANDAG provides notice that it collects, maintains, and uses location and travel pattern data in its Privacy Policy for Collection, Management, and Storage of Personal Information and Terms of Use for Online Services (Privacy Policy) and in the *FasTrak* Customer Agreement Terms and Conditions (*FasTrak* Terms and Conditions).[15]

The Privacy Policy is readily accessible by clicking "PRIVACY POLICY" on the footer of SANDAG primary webpage at sandag.org and also can be accessed on (a) the 511 San Diego Region website, 511sd.com; (b) the South Bay Expressway websites, southbayexpressway.com and sbxthe125.com; and (c) the Shift San Diego website at shiftsandiego.com.

The *FasTrak* Terms and Conditions are readily accessible from the *FasTrak* website at 511sd.com/ *FasTrak*511sd/FasTrakHome, clicking the "Get *FasTrak*" link, and

[13] See Cal.Str. & H. Code § 31490(c)-(d).
[14] See Cal.Str. & H. Code § 31490(c).
[15] Both policies are available in Spanish as well.

scrolling to the bottom of the webpage. The terms and conditions incorporate the SANDAG Privacy Policy.

2: DATA SUBJECTS' ABILITY TO ACCESS AND CORRECT THEIR INFORMATION

FasTrak subscribers and iCommute users can view their trip data, update their profile information, and change their payment methods. They also can cancel their accounts.

F: HOW SANDAG CONFIRMS THE QUALITY OF LOCATION AND TRAVEL PATTERN DATA

Whether a set of information can be relied upon to make an informed decision can be expressed as the extent to which the data is (a) available, (b) appropriate for the decision to be made, (c) regarded as correct, (d) easy to interpret and use, or (e) unbiased. Good information quality is the cornerstone for sound decisions and inspires trust in the agencies that use information.

1: TOLL DATA

SANDAG Operations Center uses (a) *FasTrak* transponder and ALPR data to determine and collect tolls and (b) video footage to monitor the toll and customer service center facilities for security and to resolve customer disputes. Transponder data quality issues are typically related to the proper attribution of a specific transponder ID to a particular vehicle or account. ALPR data quality issues relate to whether the OCR software properly "reads" each license plate. Operations Center staff visually confirm reads before issuing violation notices. Customer disputes are typically related to whether an in-lane cash or credit card transaction actually resulted in a payment.

2: TDM DATA

TDM data is not used to make any adverse determinations regarding individuals. iCommute ridesharing information, Freeway Services Patrol data, and survey responses are collected directly from the participant. Location and travel pattern data collected by ITS are based upon the location of the field sensor station. SANDAG does not check the accuracy and timeliness of TDM location and travel pattern data.

G: HOW SANDAG ENSURES THAT STAFF APPROPRIATELY MANAGES LOCATION AND TRAVEL PATTERN DATA

SANDAG senior management communicates to staff how location and travel pattern data should be managed. Those standards are set forth in SANDAG (a) board policies, (b) Employee Handbook, (c) internal operating procedures, (d) Privacy Policy, and (e) Public Records Request Guidelines.

Staff with access to PII (including location and travel pattern data) receive privacy training that emphasizes why compliance with privacy obligations is important, highlights relevant privacy risks, and provides guidance on how to address those risks. Staff is encouraged to seek clarification if they are unsure of what they should do in any situation involving the handling of personal information by discussing the issue with their supervisor or the Office of General Counsel.

The Employee Handbook states that violating SANDAG policies regarding the appropriate use of personal information can result in disciplinary action up to termination.

H: HOW SANDAG PROTECTS THE DATA

SANDAG complements its privacy policies with the safeguards discussed in Part 3(E)(2) to protect PII and confidential information, including location and travel pattern data, against unauthorized access and loss.

5

Criminal Justice Information

A: WHY SANDAG COLLECTS CRIMINAL JUSTICE DATA

SANDAG fulfills its criminal justice mission by informing and involving residents in the decision-making process on public safety issues, by promoting regional collaboration in the acquisition, maintenance, and sharing of public safety technology, and by operating ARJIS.

1: ARJIS

ARJIS was created by a Joint Powers Agreement[16] to share criminal justice information among public safety agencies to enhance their abilities to prevent and respond to crime throughout the San Diego area. ARJIS helps agencies share data by operating a database and network that makes contributing member agencies' criminal and non-criminal incident reports ("police reports") and ALPR data available to participating agencies. ARJIS also administers the Tactical Identification System (TACIDS), a facial recognition system that allows users to compare a photograph of a person taken in the field to regional arrest booking photos. TACIDS data essentially consists of (a) the arrest booking photo, (b) the facial image captured by the police official, (c) the biometric templates created by TACIDS, and (d) the results of the template comparison search.

2: CRIMINAL JUSTICE RESEARCH DIVISION

California Penal Code § 13202 authorizes SANDAG Criminal Justice Research Division ("CJ Research Division" or "Division") to access criminal offender record information (CORI) to conduct social science research including analyses of crime trends and patterns. The Division collects and uses a broad range of personal information depending upon the social issue being studied and the potential necessity to connect data across different data sources. SANDAG works to minimize collection to only necessary information based upon the study topic. Categories of data may include:

- Name
- Date of Birth
- Social Security Number
- Address
- Email
- Phone Number
- Ethnic Origin/Race
- Gender
- Sexual Orientation
- Marital Status
- Family Information

[16] California Public Utilities Code § 132354(l) authorizes SANDAG to enter into joint powers arrangements with other entities.

- Citizenship
- Census Bureau Data
- Veteran Status
- FBI Uniform Crime Reporting Data
- Police Reports
- Criminal Offender Record Information
- Employment Status and History
- Health Information
- Education Records

B: PRIVACY ISSUES RELATED TO CRIMINAL JUSTICE DATA

The risks to – and the degree of protection afforded to – an individual's PII depends upon the role they play in the criminal justice system.

1: RISKS TO VICTIMS AND WITNESSES OF CRIME

Even though victims and witnesses are not voluntary participants in the justice process, they are compelled to disclose PII to the government to further the investigation and prosecution of the crime. If a victim's PII is not properly protected, it can exacerbate their trauma, cause embarrassment, and limit their ability to heal from the experience. In instances of domestic violence, the improper release of the victim's address may make the victim more vulnerable to physical harm. A risk to witnesses is that the inappropriate release or use of their PII can make them vulnerable to physical and economic harm from persons seeking to influence their testimony.

2: RISKS TO JUVENILES

The improper handling of juvenile victims' PII may increase the victim's anxiety and obstruct their healing. Young victims may also become targets of bullying and could experience repeated victimization if they are identified as "easy targets." Child witnesses face the same risks as adult witnesses and the improper release of their identities or location information may increase their risks of suffering retaliation. The improper release of juvenile offenders' PII undermines the goals of (a) rehabilitating the juvenile, (b) guarding against the stigma of being labeled a criminal, and (b) reintegrating the juvenile into society.

3: RISKS TO ARRESTEES

Information about arrestees is made publicly available to protect against secret arrests. Releasing the fact that an individual was accused of having committed a crime when they were not convicted can damage the individual's reputation and employment prospects.

4: RISKS TO OFFENDERS

Offenders have a diminished expectation of privacy. For instance, a person convicted of a felony loses privileges including the rights to vote, serve on a jury, or bear arms. California statutes permit the public disclosure of conviction information.

5: RISKS TO THE CRIMINAL JUSTICE SYSTEM

The criminal justice process relies upon the public's trust. If justice agencies manage PII in a way that threatens victim and witness privacy, people may regard not reporting a crime or participating in a prosecution as the only alternatives to those data practices.

6: MITIGATION STRATEGIES

Risks to participants in the criminal justice system are linked to the inappropriate use and dissemination of PII. Accordingly, mitigation strategies focus on limiting who can use what information when and ensuring that those using the data are held accountable for how they use it. ARJIS, which is a law enforcement data system, follows the standards set forth in the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures, and the FBI Criminal Justice Information System (CJIS) Security Policy, both of which prohibit – and reduce users' ability to – inappropriately access and use PII. The CJ Research Division utilizes Institutional Review Board protections for research involving human subjects and complies with the confidentially requirements set forth at 28 CFR Part 22 to help ensure that PII is not inappropriately used or disseminated.

C: How SANDAG Uses and Disseminates Criminal Justice Data

1: INTERNAL ACCESS CONTROLS

Not all SANDAG personnel need access to criminal justice data to perform their jobs. Accordingly, ARJIS and the CJ Research Division:

- **Utilize role-based controls** that limit access to criminal justice data only to those staff with a need-to-know the information to perform their jobs.
- **Require that staff pass background checks** and agree in writing to comply with confidentiality requirements before accessing criminal justice data.
- **Implement on-boarding and off-boarding procedures** for granting and revoking access to criminal justice data for new and departing employees.
- **Minimize the amount of data** available to personnel to that necessary to perform the job functions.
- **Monitor and review access to data** to detect and investigate suspicious access to criminal justice data. ARJIS and the CJ Research Division take

disciplinary action against personnel who inappropriately access criminal justice data.

Additionally, ARJIS implements the internal access controls required by the FBI CJIS Security Policy and the CLETS Policy.

2: DISSEMINATION OF THE DATA OUTSIDE OF SANDAG

ARJIS and the CJ Research Division prohibit staff with access to criminal justice data from disclosing it without authorization and emphasize that unacceptable use of the data carries significant penalties up to termination.

ARJIS's primary role is to make the criminal justice data provided by contributing member agencies available to ARJIS member agencies on a case-by-case basis. ARJIS member agencies are prohibited from disseminating ARJIS criminal justice data to other agencies. A member agency that receives a request for information that it does not own cannot release that information but rather refers the requestor to the contributing member agency that is the source of the information.

The CJ Research Division disseminates project findings to the public. Those findings do not contain PII of any data subjects. The Division does not transfer data outside of SANDAG in identifiable form.

D: HOW LONG SANDAG AND ARJIS KEEPS CRIMINAL JUSTICE DATA

The retention periods for criminal justice data are set forth in SANDAG records retention schedule. Generally, the CJ Research Division destroys the PII of data subjects at the conclusion of each research project, but in some instances, it keeps scrubbed data permanently. SANDAG Records Management Policy requires records containing PII or confidential information to be disposed of (a) promptly upon the expiration of their retention period, and (b) in a manner that does not disclose their content.

E: HOW THE PUBLIC IS MADE AWARE OF SANDAG PRACTICES REGARDING CRIMINAL JUSTICE DATA

1: NOTICE OF AND CONSENT TO COLLECTION OF CRIMINAL JUSTICE DATA

The consumer transaction model of notice and consent does not transfer to the criminal justice context because victims, witnesses, arrestees, and offenders are not voluntary participants in the justice system and are compelled to release PII to law enforcement agencies. Nevertheless, ARJIS provides notice that it collects, maintains, and uses criminal justice data on its webpage at arjis.org. There, the public can access the ARJIS Joint Powers Agreement and the Memorandum of Understanding that SANDAG, ARJIS, and the ARJIS member agencies have entered into. The ARJIS webpage also contains the Acceptable Use Policies for Law Enforcement LPR Data and the TACIDS facial recognition system.

When the CJ Research Division utilizes data it collects through its own data-collection tools (such as direct observation, interviews, and surveys),[17] data subjects complete an informed consent form that (a) discusses the nature of the research being conducted, (b) explains that the data will only be used for research or statistical purposes, and (c) states that participating in the research is not mandatory and that the data subject can stop participating at any time.

2: DATA SUBJECTS CANNOT ACCESS OR CORRECT THEIR CRIMINAL JUSTICE INFORMATION

ARJIS does not provide data subjects an opportunity to access or correct criminal justice data because it does not own most of the data it maintains and disseminates to its member agencies and therefore cannot make changes to that data. Police reports and Law Enforcement LPR Data remain the property and responsibility of the agency that contributed the data. The only data contained in the TACIDS facial recognition system owned by ARJIS is the facial template data created by the software used to compare photos.

SANDAG does not provide data subjects an opportunity to access or correct the criminal justice data they provide to the CJ Research Division. In many instances, data subjects are the source of the data collected by the Division and there is no need to correct the data. Other times, the data subject's identifying information has already been scrubbed and it would be impossible to retrieve the data subject's record for purposes of correcting their information

The inability to access and correct criminal justice information does not negatively impact data subjects because the data is not used to make adverse determinations. For instance, research data is aggregated to detect crime trend and measure the effectiveness of crime policies. Similarly, TACIDS does not positively identify individuals but rather creates templates from photographs to calculate how similar an individual's facial image is to an arrest booking photo uploaded to the system.

F: HOW SANDAG CONFIRMS THE QUALITY OF CRIMINAL JUSTICE DATA

Each ARJIS member agency retains control, ownership, and data quality responsibilities as to the data it submits to ARJIS. The performance of TACIDS is impacted by variability in the facial images caused by a number of factors including (a) the subject's age, environment, expression and, stress; (b) the camera's age, calibration, and compensation for ambient light, and (c) the matching algorithm. Since TACIDS is not relied upon to positively identify individuals, ARJIS does not take any data quality responsibilities for the data.

[17] The Division also uses ARJIS data.

The CJ Research Division's data quality responsibilities are tied to the data collection process and how accurately the data is entered into software programs that help analyze the data. Data collection and entry is checked for accuracy during the course of each study.

G: HOW SANDAG ENSURES THAT STAFF APPROPRIATELY MANAGES CRIMINAL JUSTICE DATA

SANDAG senior management communicates to ARJIS and CJ Research Division staff how criminal justice data should be managed. Those standards are set forth in SANDAG (a) board policies, (b) Employee Handbook, (c) internal operating procedures, (d) Privacy Policy, and (e) Public Records Request Guidelines. The Employee Handbook states that violating SANDAG policies regarding the appropriate use of PII or confidential information can result in disciplinary action up to termination.

1: ARJIS

ARJIS requires its member agencies to train its personnel prior to allowing them to access and use ARJIS criminal justice data. Training must include the subjects set forth in the CLETS Policy, which incorporates the security awareness training requirements at Section 5.2 of the FBI CJIS Security Policy. Because it is an active law enforcement data system, ARJIS must comply with federal privacy and security requirements and is audited by the FBI and the California Department of Justice.[18]

ARJIS automatically logs users' access to and use of criminal justice data. Those logs are maintained for three years and include (a) the user's name and agency, (b) the date and time of access, (c) the specific data queried, and (d) the justification for the inquiry, including the case number if available. SANDAG Director of Technical Services can suspend any ARJIS member agency's account if it is determined that ARJIS criminal justice data has been misused.

2: CJ RESEARCH DIVISION

The Director of the CJ Research Division oversees the protection of criminal justice research subjects. For research funded by the U.S. Department of Justice, the Division follows the privacy requirements set forth in 28 CFR Part 22 and is subject to external audits by research partners. Moreover, CJ Research Division Staff receive in-person training regarding the appropriate handling of criminal justice data and are required to sign a confidentiality agreement before they access any PII.

[18]See CLETS Policy and Security Audit Questionnaire.

H: HOW SANDAG PROTECTS THE DATA

In addition to the safeguards discussed in Part 3(E)(2), ARJIS and the CJ Research Division implement the following.

1: ARJIS

ARJIS and ARJIS member agencies must comply with the FBI Criminal Justice Information System (CJIS) Security Policy and the California Department of Justice California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures, which contain comprehensive security safeguards for protecting criminal justice data.

To implement these requirements, ARJIS secures its member agencies' data by (a) using multi-factor authentication, (b) requiring complex passwords, (c) encrypting communications, (d) setting up firewalls, and (e) recording audit logs. Moreover, ARJIS servers containing criminal justice data are stored in a secure law enforcement facility. Access to ARJIS data is limited to ARJIS IT staff and police officials employed by ARJIS member agencies.

2: CJ RESEARCH DIVISION

The Division maintains its own written security procedures which are provided to research staff and require that (a) electronic files containing PII be saved on secure servers or in "Restricted Data" folders in an encrypted format, (b) disks containing unencrypted data and hardcopies of documents containing PII to be kept in a locked file cabinet when not in use, (c) staff lock or log out of their computers before leaving them unattended, (d) PII saved temporarily on computer hard drives be deleted and (e) staff consult with the project manager before copying data. The procedures also prohibit staff from taking data containing PII home or discussing the contents of files containing confidential information with anyone other than research staff.

6

Consumer Information

A: WHY SANDAG COLLECTS CONSUMER INFORMATION

SANDAG aims to increase commuter awareness of – and participation in – TDM and TSM programs to reduce demand on the transportation network. SANDAG collects information about the traveling public through its outreach and marketing programs.

1: WEBSITE VISITORS AND SOCIAL MEDIA USERS

SANDAG collects information from individuals when they visit the online services it hosts including (a) the Internet domain and IP address used to access the website, (b) the type of browser and operating system used to access the website, and (c) clickstream data, such as the date and time the webpage was accessed, the webpages visited, and whether the visitor accessed SANDAG website from another website and, if so, that website's address. SANDAG also uses cookies to improve visitors' experience on the website. This data allows SANDAG to assess how visitors use its website and gives insights such as which pages are most popular, what content attracts the most attention, and where visitors spend their time so that SANDAG can improve the website experience.

SANDAG Communications Division utilizes social networking websites (e.g., Facebook, Twitter, and YouTube) to disseminate information to the public and to promote SANDAG news and resources to social media users who may not be regular visitors to SANDAG primary website. The PII available to SANDAG via social networking websites comes from individual users. SANDAG does not use social networking websites to collect, use, or retain PII from any individual. Nevertheless, SANDAG may read or use information that users make available to SANDAG on a social networking website, including comments on SANDAG pages or posts.

2: MAILING LISTS AND PUBLIC WORKSHOPS

As the region's transportation planning agency, SANDAG creates opportunities for engaging the public by publishing newsletters, holding public workshops and meetings, making presentations to community groups, and posting documents online to solicit comments. Individuals may provide SANDAG with their name and contact information to (a) receive newsletters, (b) sign in at workshops and meetings, or (c) submit questions or comments.

Information provided to SANDAG as part of the public outreach process becomes a public record and, as such, may be publicly disclosed pursuant to the California Public Records Act. Certain records, however, may be withheld from public inspection where it is necessary to protect a data subject's personal privacy, to

allow SANDAG to negotiate effectively, and to obtain legal advice. Accordingly, whenever a request is made for records that are protected by the Public Records Act, SANDAG denies the request and identifies the portion of the law that allows it to withhold the requested records. Please see SANDAG Board Policy 015: Records Management Policy for more information regarding public records.

B: PRIVACY ISSUES RELATED TO CONSUMER INFORMATION

Clickstream data has the potential to reveal insights into a particular visitor's web browsing habits. SANDAG mitigates this risk by aggregating clickstream data so it is not individually identifiable, making it available only to staff with a need to know the information, and only using the data internally to assess SANDAG efforts to engage the public and improve the website. Additionally, SANDAG limits access to IP address information to specifically authorized staff and prohibits staff from using website traffic data to track the activity of individual users.

SANDAG use of social networking websites creates minimal risks to individual privacy. Users register for social networking accounts, set their own privacy settings, and select what information to add to their public profiles. All of their data is maintained by the social networking website administrator, not SANDAG. One risk is that a user includes PII or other sensitive personal information in a comment posted to SANDAG page.

The impact of SANDAG direct mailing and workshop attendance lists on individual privacy is also low. The lists contain voluntarily submitted names, email addresses, and physical addresses. The privacy risk is that an individual's name and contact information are improperly accessed or used. To mitigate this risk, SANDAG policies limit access to the lists to authorized SANDAG staff with a need to know the information and SANDAG does not disseminate contact information to unrelated third parties without the individual's consent or unless required by law.

C: HOW SANDAG USES AND DISSEMINATES CONSUMER INFORMATION

1: INTERNAL ACCESS AND USE OF THE DATA

Aggregated clickstream data that is not individually identifiable is used to assess SANDAG efforts to engage the public and to improve the website. On social networking websites with SANDAG webpages, staff may (a) read or act upon information provided by individuals in comments, (b) answer questions from users, (c) host interactive events, and (d) conduct media research by searching websites for agency mentions. SANDAG also may use non-individually-identifiable analytical data made available by social networking websites to measure public engagement with SANDAG.

SANDAG uses individuals' names and contact information to (a) send requested publications or communications, (b) contact them in the event of delivery

problems, (c) respond to questions and comments, and (d) provide and improve TDM, TSM, and other transportation programs.

2: DISSEMINATION OF THE DATA OUTSIDE OF SANDAG

In the absence of a law requiring SANDAG to do so,[19] it does not disseminate to entities or persons unrelated to SANDAG (a) aggregated clickstream data, (b) PII made available to it on social networking websites, or (c) individuals' names, telephone numbers, email addresses, subscription information, or opt-in status. Comments posted on SANDAG social networking webpages are publicly available to anyone visiting SANDAG pages.

D: HOW LONG SANDAG KEEPS CONSUMER INFORMATION

The retention periods for consumer information are set forth in SANDAG records retention schedule. SANDAG Records Management Policy requires records containing PII or confidential information to be disposed of (a) promptly upon the expiration of their retention period, and (b) in a manner that does not disclose their content.

E: HOW THE PUBLIC IS MADE AWARE OF SANDAG PRACTICES REGARDING CONSUMER INFORMATION

SANDAG website contains a link to its Privacy Policy, which identifies the information automatically collected from website visitors and how it is used. Social networking websites are run by third parties that are each responsible for notifying data subjects that their data is being collected and determining whether to extend to data subjects the ability to access and correct PII about them.

Individuals may decline to provide their names and contact information to SANDAG, but requests for SANDAG publications and newsletters cannot be processed without the information. Customers who choose to receive SANDAG communications but then later decide that they no longer wish to receive them may contact SANDAG to unsubscribe from SANDAG contact lists.

F: HOW SANDAG CONFIRMS THE QUALITY OF CONSUMER INFORMATION

SANDAG does not check the accuracy and timeliness of (a) clickstream data automatically collected as part of running its websites or (b) PII from individuals

[19] For example, the SANDAG may receive requests for consumer information pursuant to the California Public Records Act (CPRA). The CPRA, however, exempts from public disclosure documents "the disclosure of which would constitute an unwarranted invasion of personal privacy." See Cal. Gov. Code § 6254(c). SANDAG does not disseminate to the public records that are exempt from the CPRA. Also, the California Environmental Quality Act requires SANDAG environmental impact reports to contain the name and contact information of individuals who commented upon draft reports. See 14 Cal. Code Regs. Tit. 14 § 15129.

who visit SANDAG social networking webpages. SANDAG may process mailing addresses through a verification system to validate the street address, city, state, and ZIP code.

G: HOW SANDAG ENSURES THAT STAFF APPROPRIATELY MANAGES THE CONSUMER INFORMATION

SANDAG senior management communicates to staff how consumer information should be managed. Those standards are set forth in SANDAG (a) board policies, (b) Employee Handbook, (c) internal operating procedures, (d) Privacy Policy, and (e) Public Records Request Guidelines.

Employees with access to individually identifiable consumer information receive training on how to implement SANDAG Privacy Policy as well as its Social Media Terms of Use. Staff is encouraged to seek clarification if they are unsure of what they should do in any situation involving the handling of personal information by discussing the issue with their supervisor or the Office of General Counsel.

The Employee Handbook states that violating SANDAG policies regarding the appropriate use of personal information can result in disciplinary action up to termination.

H: SECURITY SAFEGUARDS PROTECTING THE DATA

Each social networking website, not SANDAG, controls the security of comments and other information posted on that site. Accordingly, SANDAG does not implement security safeguards with respect to social media user information. With respect to other consumer information SANDAG complements its privacy policies with the safeguards discussed in Part 3(E)(2) to protect PII and confidential information, including consumer information, against unauthorized access and loss.

7

Glossary

ARJIS member agencies include contributing member agencies and participating member agencies.

An **Arrestee** is an individual who was arrested and charged with the commission of a crime but (a) was not convicted, (b) had his conviction overturned on appeal, or (c) was released by police without formal charges being filed.

The term **Comments** includes information, pictures, videos, articles, and other content posted on a SANDAG social networking webpage.

Contributing member agency is the law enforcement agency that creates, submits, or modifies police incident report data contained in ARJIS.

Disseminating data means providing the recipient with a copy of information and retaining the original data.

Police report data refers only to police incident reports submitted to and contained in ARJIS on the day the information is accessed or disseminated. The phrase does not refer to the actual police incident reports maintained at contributing member agencies. This negates the need to say, "police incident reports contained in ARJIS."

Need to know is the standard whereby an authorized user is granted access to information because they have a clearly ascertainable business reason for accessing the data.

An **Offender** is an individual who has been convicted of committing a crime.

Participating member agency is the law enforcement agency that does not contribute police incident report data to ARJIS but can access ARJIS data and services.

Personally Identifiable Information (PII) is information about an individual that distinguishes or traces an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; or is linked or linkable to an individual, such as medical, educational, financial, and employment history. Source: Erika McMallister et al., NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information §2.1 (2010).

Police officials means all manner of law enforcement officers including peace officers, federal law enforcement officials, state police, municipal police, and sheriffs.

Sharing data means allowing the recipient to view the information without giving that person a copy of the information.

Third party service providers (Providers) are outside, unrelated organizations that provide SANDAG with consulting, legal, real estate, education, communications, storage, processing, and many other types of services.

Transferring data means providing information to a third party without retaining a copy of the information.

Appendix A
Scrubbing Data

The terms "anonymized" and "de-identified" are often used to imply that the data they describe cannot be re-identified. This is not always true. Instead of using a word that implies an incorrect result, this report uses the term "scrub" to describe privacy-motivated data manipulation that connotes an effort to protect privacy, even if the effort is not ultimately successful.

Scrubbing is the process by which information in a database is manipulated to make it difficult to identify data subjects. There are several approaches, algorithms, and tools that can be applied to different kinds of data with differing levels of effectiveness.[20]

Generally, to scrub a dataset, the database administrator singles out identifying fields and then: (a) removes the fields from the table altogether, (b) alters the field values to make the value more generalized (e.g., by truncating ZIP codes to three digits), or (c) releases only summary statistics, not raw data.

The method used to scrub information is important because 87 percent of people in the U.S. can be uniquely identified by their combined five-digit zip code, birthdate (including year), and gender.[21] In contrast, when the birthdate is generalized to only include the year of birth and the ZIP code is truncated to three digits, less than 1 percent of records can be re-identified.[22]

[20] Simson L. Garfinkel, De-identification of Personal Information (NISTIR 8053), October 2015 at 1.
[21] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701, 1705 (2010).
[22] Simson L. Garfinkel, De-identification of Personal Information at 25.

Appendix B

California Statutes Protecting Addresses

Group	Statute	Synopsis
Victims: **Sex Crimes**	Cal.Gov.Code § 6254(f)(3); Cal.Pen.Code § 293(c); Cal.Gov.Code § 6205 *et seq.*	A law enforcement agency shall not disclose the address of a person who alleges to be the victim of a sex offense to any person other than prosecutors, parole officers, parole hearing officers, probation officers, or other statutorily authorized persons.
Victims: **Domestic Violence**	Cal.Gov.Code § 6205 *et seq*.	State and local agencies may respond to requests for public records without disclosing the location of a domestic violence victim.
Victims: **Stalking**	Cal.Gov.Code § 6205 *et seq*.	State and local agencies may respond to requests for public records without disclosing the location of a stalking victim.
Victims or Witnesses	Cal.Pen.Code § 964(a)	The district attorney, the courts, and local law enforcement agencies must establish a procedure to protect confidential personal information regarding any witness or victim contained in a police report if the report is submitted to a court to support a complaint, indictment, information, or warrant. Information related to any victim or witness receiving notice from the Department of Corrections and Rehabilitation or Board of Parole Hearings concerning the release, escape, or death of an offender is confidential and is not subject to disclosure under the California Public Records Act.
Elected or Appointed Officials	Cal.Gov.Code § 6254.21(a)-(d); Cal.Elec.Code §2166.7(a)	Limits posting the home address of any elected or appointed official or family member on the Internet.
Marriage License Parties or Witnesses	Cal.Fam.Code § 351.5	Any applicant for or witness to a marriage certificate or license can request to use their business address instead of their home address.

Group	Statute	Synopsis
Candidates for Judicial Office	Cal.Elec.Code § 8023(c)	No candidate for a judicial office shall be required to state his or her residential address on the declaration of intention.
Voters	Cal.Elec.Code § 2194(a)(1)	Affidavits of voter registration information shall be confidential and shall not appear on any computer terminal, list, or other medium available to the public at the county elections official's office for a period of 100 years.
Driver's License or State Identification Card Applicants	18 U.S. Code § 2721(a)(1); Cal.Veh.Code § 1808.21(a); Cal.Civ.Code § 1798.24	Residence addresses in any record of the DMV is confidential and shall not be disclosed to any person, except a court, law enforcement agency, or other government agency.
Reproductive Health Services Facility Provider, Employee, Volunteer, or Patient	Cal.Gov.Code § 6218(a)(1)	No person or entity shall publicly post on the Internet the home address of any provider, employee, volunteer, or patient of a reproductive health services facility or other individuals residing at the same home address with the intent to incite a third person to threaten or cause bodily harm to the person identified in the posting.

Appendix C

Issues Outside the Scope of This Report

1: CONNECTED OR AUTOMATED VEHICLES

Connected vehicles that communicate with other vehicles and with infrastructure can improve (a) safety by providing warnings to drivers, pedestrians and bicyclists, about potential crash situations, such as when a vehicle two cars ahead brakes suddenly, or when a vehicle is on a collision course with a pedestrian, (b) mobility by providing information about traffic conditions so drivers can make informed travel decisions, and (c) the environment by providing real-time information to travelers to help eliminate unnecessary stops and reduce congestion.

Self-driving vehicles utilize internal sensors to survey and respond to the surrounding transportation environment including other vehicles and pedestrians.

The San Diego region has been designated by the U.S. Department of Transportation as a proving ground for connected and automated vehicles.[23] It is not yet known what data may be collected as part of the testing activities associated with the designation. The privacy issues related to those testing activities will be discussed by a separate report as part of the tests.

2: BUS ON SHOULDER

SANDAG Bus on Shoulder (BOS) project will provide a time competitive transit alternative for travel. In addition to shoulder lane improvements, the project will use lane-keeping technology to provide additional safety enhancements and blind spot warnings so that buses can safely navigate between the express lanes and the shoulders and ultimately enhance the overall safety of vehicle operations. The project proposal also includes a ramp signal that would use real-time vehicle location information to hold approaching vehicles at ramp meters and allow buses to utilize the outside freeway shoulder, resulting in reduced conflicts between buses and merging vehicles. It is not yet known what data may be collected as part of the BOS project. SANDAG will address the privacy issues related to the BOS project separately.

3: CREDIT AND DEBIT CARD INFORMATION

SANDAG collects credit and debit card information to process payments for SANDAG services. The security guidelines for handling credit and debit card information – the Payment Card Industry Data Security Standard (PCI DSS) – are mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard requires increased security around

[23] Marianne Kushi, How San Diego County Could Be Testing Ground for Autonomous Cars, NBC San Diego (May 9, 2016).

cardholder data to reduce credit card fraud. SANDAG has engaged the services of another consultant to ensure that its practices meet or exceed the industry standards.

4: CONSTRUCTION CONTRACT INFORMATION

In its administration of the *TransNet* program, SANDAG collects from contractors certified payroll information that contains the PII (including name, address, and social security number) of the contractors' employees. SANDAG redacts addresses and Social Security numbers when responding to requests made under the California Public Records Act.