The California Values Act: Guidelines to Protect Personal Information in Law Enforcement Databases

Community Stakeholder Recommendations

July 2018

I. Executive Summary

As organizations that work to protect the rights, privacy, and security of all California residents regardless of immigration status, we have long studied the sharing of personal information among state, local, and federal agencies for the purposes of immigration enforcement. Databases operated by law enforcement agencies serve as a critical method by which federal immigration enforcement agencies detect and detain individuals. The California Values Act addresses the sharing of personal information for immigration enforcement purposes by placing strict limits on law enforcement agencies engaging in immigration enforcement and by protecting the personal information of California residents to the maximum extent possible. Cal. Gov't Code §§ 7282 *et seq*. To implement these protections, the California Attorney General is required to "publish guidance, audit criteria, and training recommendations" for limits to the availability of personal information in law enforcement databases for immigration enforcement purposes. *Id.* § 7284.8(b). We offer specific recommendations on guidelines and procedures that law enforcement agencies should adopt to ensure that personal information in databases is not used for immigration enforcement purposes.

Drawing from the Fair Information Practice Principles, our key recommendations include:

- Agencies should **limit collection** of personal information that could be used for immigration enforcement purposes, such as place of birth, tax numbers, and addresses.
- Agencies should enact safeguards to comply with the California Values Act and **prohibit sharing** of personal information with internal and external entities for the purposes of immigration enforcement, including procedures for determining legitimate and permissible purposes of requests for that information and requiring certification that the information will not be used for immigration enforcement.
- Any authorized and permitted sharing of personal information should be on an **individualized basis, logged, recorded, and routinely audited**.
- Agencies should issue **privacy and usage policies** for each of its databases, outlining the personal information held in those databases, the authorized and permissible forms, methods, and process of sharing of information with internal and external entities, and the policies for auditing the sharing of that information to ensure that it complies with the agency's policies.
- Specific safeguards should be adopted for personal information transmitted through the California Law Enforcement Telecommunications Network ("CLETS"), collected by the California Department of Motor Vehicles, handled by California fusion centers, collected using surveillance technologies, or contained in gang databases.

We define "personal information" to include any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

We define "database" to include a set of records of any sort – text, images, etc. – whether held electronically or otherwise that can be queried to retrieve records matching certain criteria.

II. California Law Supports Robust Protection of Individual Privacy

Californians enjoy robust protection under state and federal law for the privacy of their personal information. Not only does the California Constitution enshrine a right to privacy, a range of statutory provisions circumscribe sharing of personal information.

All people in California possess a right to privacy protected by Article I, Section 1 of the California Constitution. "Informational privacy" is one of the rights enjoyed by individuals and encompasses an individual's interest in "precluding the dissemination or misuse of sensitive and confidential information." *Hill v. Nat'l Collegiate Athletic Assn*, 7 Cal.4th 1, 35 (1994). Among other purposes, Article I, Section 1 is intended to prevent "the overbroad collection and retention of unnecessary personal information by government and business interests" and "the improper use of information properly obtained for a specific purpose, for example, . . . the disclosure of it to some third party." *White v. Davis*, 13 Cal.3d 757, 775 (1975).

The Information Practices Act ("IPA") provides further protections for individual privacy. Recognizing that the right to privacy is threatened by "indiscriminate collection, maintenance, and dissemination of personal information," the IPA imposes "strict limits" on the maintenance and dissemination of that information. *See* Cal. Civil Code §§ 1798.1(a), (c). State agencies are generally prohibited from releasing an individual's personal information except in narrow statutorily-specified circumstances. *See id.* § 1798.24.

Specific types of personal information—such as criminal history and court records—are subject to even more stringent protection under California law. In compiling and maintaining an individual's criminal history or "criminal offender record information" ("CORI"), criminal justice agencies are "restricted to that which is recorded as the result of an arrest, detention, or other initiation of criminal proceedings or of any consequent proceedings related thereto." Cal. Penal Code § 13102. An agency may only release CORI to individuals and entities specified in the Penal Code in certain circumstances. *Id.* §§ 11105; 13300. The requesting person or agency must (1) be authorized by either a court order, statute, or case law to receive the information (*right-to-know*), and (2) have a compelling reason to request the information to execute their official responsibilities (*need-to-know*).

California law also prohibits the public disclosure of certain information contained in court records. *See generally* Judicial Council of California, Trial Court Records Manual at 69-78 & App. 1, Jan. 1, 2018, https://bit.ly/2IJsIUV. Among the records that must be maintained as confidential are the immigration status of a child in Special Immigration Juvenile Status proceedings, certifications provided to beneficiaries of U visas, juvenile court records regardless of a juvenile's immigration status, social security numbers and financial account numbers. *See id.* at 73-74. The California Rules of Court issued by the Judicial Council of California prohibit several pieces of information from being included in a court's electronic calendar, index or register, including social security information, ethnicity, driver's license number, and date of birth. *See* Cal. Rule of Court § 2.507(c).

Recent legislation in California enacts protections that recognize the significant privacy interests held by immigrants in their personal information. There is a complex web of databases, related systems, and information-sharing mechanisms that facilitate immigration enforcement activities by drawing on

personal information held in state and local databases.[1] To address these concerns, the California Values Act prohibits state and local law enforcement agencies from using money or personnel for "immigration enforcement purposes," subject to certain exceptions. Cal. Gov't. Code § 7284.6(a)(1). The statute defines "immigrant enforcement" broadly to include not only the investigation and enforcement of *civil* immigration law, but also the investigation and enforcement of "*criminal* immigration law that penalizes a person's presence in, entry, or reentry to, or employment in, the United States." *Id.* § 7284.4(f). To implement these protections, state and local law enforcement agencies are prohibited from inquiring into an individual's immigration status. *Id.* § 7284.6(a)(1)(A). They are also prohibited from providing personal information about an individual, including but not limited to an individual's home or work addresses, for immigration enforcement purposes, unless that information is available to the public. *Id.* § 7284.6(a)(1)(D). "Personal information" broadly encompasses any information that "identifies or describes an individual," including but not limited to their name, place of birth, social security or other taxpayer identification number, home and work addresses, and employment history. *See* Cal. Civil Code § 1798.3(a).[2]

The California Values Act does not prohibit or restrict law enforcement agencies from sharing information about an individual's immigration or citizenship status, a provision that was included to ensure that the act did not violate 8 U.S.C. § 1373. *Id.* § 7284.6(e). However, the constitutionality of 8 U.S.C. § 1373 has been called into question by recent court decisions. In its opinion striking down a federal statute that prohibited states from repealing their sports gambling laws, the Supreme Court held that Congress may not "issue direct orders to the governments of the States" and that that same principle applies to orders either to "enact or refrain from enacting state law." *Murphy v. Nat'l Collegiate Athletic Ass'n*, 2018 WL 2186168, 15, 19 (U.S. May 14, 2018). The logic of *Murphy* extends to 8 U.S.C § 1373, which prohibits States from enacting laws restricting the sharing of information about an individual's immigration or citizenship status. A federal district court, citing *Murphy*, held that 8 U.S.C. § 1373 is unconstitutional under Tenth Amendment. *See City of Philadelphia v. Sessions*, 2018 WL 2725503, at *32-33 (E.D. Pa. June 6, 2018); *cf. United States v. California*, 2018 WL 3301414, at *14 (E.D. Ca. July 5, 2018) (finding constitutionality of Section 1373 "highly suspect").

In addition to the Values Act, the Transparent Review of Unjust Transfers and Holds ("TRUTH") Act requires fair notice to be provided to immigrants if and when California law enforcement agencies receive a hold, notice and/or transfer request from U.S. Immigration and Customs Enforcement ("ICE"). Cal. Gov't Code § 7283.1(b). Law enforcement agencies must also notify the individual of whether they will honor the request or not, additionally providing notice to the individual's attorney or designee in instances of a notice request. *Id*. And most recently, the Governor signed S.B. 785 into law to prohibit the disclosure of an individual's immigration status in open court unless the presiding judge first determines the evidence is admissible in an *in camera* hearing. *See* Cal. Evidence Code §§ 351.3, 351.4.

---

[1] *See* National Immigration Law Center, Untangling the Immigration Enforcement Web: Basic Information for Advocates About Databases and Information-Sharing Among Federal, State, and Local Agencies (Sept. 2017); Electronic Frontier Foundation, From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond (May 2012).

[2] While state and local law enforcement agencies cannot inquire into immigration status and cannot provide non-public personal information about an individual, they may provide information about a specific person's criminal history to immigration authorities, where it is otherwise permitted by state law and does not violate any local law or policy. *See* Cal. Gov't Code § 7284.6(b)(2).

III. The Fair Information Practice Principles Protect Data Held in Law Enforcement Databases

The guidelines for law enforcement databases should conform to a privacy framework such as the Fair Information Practice Principles ("FIPP"), an internationally-recognized set of principles that inform informational privacy policies and incorporate individual privacy considerations. The FIPPs have been adopted by the federal government as its general policy and guiding principles for managing and evaluating systems, processes, and activities that affect individual privacy and involve personally-identifiable information ("PII").[3] While the articulation of the FIPPs have varied and evolved, there are a set of core principles addressing the following aspects of data management: collection, disclosure, secondary usage, record correction, and security.

One example among the various federal agencies that have implemented the FIPPs is the U.S. Department of Homeland Security's ("DHS") privacy policy.[4] Though the DHS's privacy policy does not include all protections we would recommend as part of the law enforcement database guidelines, it serves as an important reference here. DHS operates databases containing PII of U.S. citizens, Lawful Permanent Residents ("LPR"), and other individuals who are not citizens or LPRs. In 2007, DHS announced that all persons' PII, regardless of citizenship, would be treated and receive the same protections under the federal Privacy Act. After President Trump issued an Executive Order in January 2017 directing agencies not to extend the protections of the Privacy Act to anyone other than citizens and LPRs, DHS stated it would begin treating all persons, regardless of immigration status, consistent with the FIPPs and applicable law.[5]

DHS has articulated the following FIPPs as governing its information practices: (1) purpose specification; (2) data minimization; (3) use limitation; (4) individual participation; (5) data quality and integrity; (6) security; (7) accountability and auditing; and (8) transparency.

The Purpose Specification principle requires agencies to possess clear, legally-authorized purposes for collecting each piece of personal information. Further, any planned purpose for the collected piece of personal information should be compatible with the original purposes for which the information was collected. For example, DHS declines to collect personal information in the absence of legal authority to act on the information. *See* DHS Privacy Guidance at 4. Further, DHS must articulate in its public notices the authorities that permit the collection of information about individuals in DHS databases, the purposes for which the information is intended to be used, and the compatibility between the intended purposes and the purpose for which DHS originally collected the information.

Under the Data Minimization principle, agencies can collect information only that is relevant and necessary to accomplish the purposes specified, and can retain that information only as long as is necessary to fulfill those purposes. DHS, for example, does not collect, use, maintain, or disseminate social security numbers unless legally required or for a specific authorized purpose. *See* DHS Privacy

[3] U.S. Office of Management & Budget, Appendix I to OMB Circular No. A-130: Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016), https://obamawhitehouse.archives.gov/omb/circulars_default.
[4] *See* U.S. Dep't of Homeland Security, Privacy Policy Guidance Memorandum 2017-01 at 3, Apr. 27, 2017, https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.
[5] *Id.* at 1.

Guidance at 5. Further, DHS notes the risks inherent in collecting data specifically targeted at determining citizenship status and notes that only needed data elements should be collected.

The Use Limitation principle limits agencies to using personal information for the purposes specified in published privacy notices. In the context of sharing personal information with other agencies, DHS has adopted several relevant policies to ensure that sharing is authorized, justified, and purpose-compatible. DHS must confirm whether an agreement, federal statute, or other legal authority authorizes sharing of personal information and must follow the terms of that agreement or arrangement when sharing information. *See* DHS Privacy Guidance at 9. Even where sharing is legally permitted, DHS must review any other policy considerations that would affect the decision to share information. DHS must confirm that "any sharing of such information outside the agency must be compatible with the purposes for which the information was originally collected." *Id.* at 5. In some instances, DHS can only share personal information with the written consent of the individual. Where sharing occurs, DHS requires the receiving agency to protect against further dissemination of those records. DHS must describe and justify all sharing that relates to immigrants and nonimmigrants, and identify the categories of internal and external entities with which it shares personal information.

The Individual Participation principle ensures that an individual is involved in determining how his or her personal information is used. For example, DHS seeks an individual's consent, to the extent practicable, for the collection, use, dissemination, or maintenance of personally-identifying information. *Id.* at 4. Further, where not otherwise prohibited, DHS permits individuals access to records containing their personal information in order to contest the accuracy of the information or to update or amend records, such as the Traveler Inquiry Redress Program. As DHS notes, "allowing people to update and amend records can reduce unnecessary errors, improve effectiveness and outcomes, and prevent waste at partner agencies that often rely on the same information." *Id.* The federal Privacy Act and the California Information Practices Act also provide individuals a statutory right to amend records containing their personal information that are held by federal and state agencies, respectively. *See* 5 U.S.C. § 552a(d); Cal. Civil Code § 1798.34. The California TRUTH Act requires law enforcement agencies to provide fair notice to immigrants upon receiving a hold, notice and/or transfer request from ICE, and whether the agency will honor the request. *See* Cal. Gov't Code § 7283.1(b).

The Data Quality and Integrity principle ensures that agencies rely on information that is reasonably considered accurate, relevant, timely, and complete.

The Security principle requires agencies to protect personal information from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

To implement the Accountability and Auditing principle, agencies must engage in processes to ensure their handling of personal information comport with the applicable law and policies. For example, DHS uses training of its employees and contractors that have access to personally-identifying information, alongside investigations of privacy policy violations and privacy reviews of its systems, to ensure that it is accountable for the use of information collected, maintained, and used in its systems. *See* DHS Privacy Guidance at 7.

The Transparency principle requires agencies to publish notices, privacy impact assessments, or other public documents outlining how it handles personal information.

IV. Guidelines for Protection of Immigrant Data in Law Enforcement Databases

Drawing from the FIPPs, we recommend that law enforcement agencies implement policies and practices that are tailored towards ensuring that personal information held in their databases is not used for immigration enforcement purposes.

We recommend that these guidelines be adopted not only by county sheriff's offices and local police departments that operate databases directly or through private vendors, but also other law enforcement agencies at the city, county, and state levels, such as district attorney's offices or probation offices, that operate, participate, or contribute information to federal, state-wide, county-wide or local criminal justice databases or networks.

Purpose Specification and Data Minimization

- *Limit Collection*. To prevent law enforcement databases from being used for immigration enforcement purposes, agencies should limit wherever possible the collection of personal information that could be used for those purposes. Under the California Values Act, agencies are prohibited from inquiring into immigration status. Agencies should also avoid collecting other information from individuals that could be used for immigration enforcement purposes as a proxy for immigration status, such as place of birth, employment information, social security number or lack thereof, tax identification number, or home or work address, unless (1) the agency is authorized under law to collect and act upon the information; and (2) the agency has a legally-authorized purpose for collection of this information.

- *Consider Alternative Methods*. If agencies have legal obligations necessitating inquiry into place of birth, tax numbers, or employment information, they should consider alternate methods of fulfilling these obligations that would not require collecting sensitive personal information that could later be used for immigration enforcement. For example, to meet mandatory consular notification obligations as outlined under Cal. Penal Code § 834c(d) for foreign nationals that are arrested, law enforcement agencies could present arrested individuals with the list of the 56 enumerated countries and check whether notification is required instead of asking individuals where they were born or what their country of citizenship is.

- *Limit (Electronic) Retention*. If agencies collect information about place of birth, tax numbers, or employment, they should minimize maintenance of this information in recorded form, including hard copy forms or in electronic databases. Agencies should also adopt retention periods no longer than is necessary to fulfill the purpose justifying collection of the information. Further, they should consider whether databases can be configured to redact or purge personal information after the purpose for its collection has been achieved or after a specific amount of time has passed; to limit its availability to certain, specified users; or to otherwise limit its availability for immigration enforcement purposes.

Use Limitation and Individual Participation; Security and Data Quality and Integrity

- To ensure that personal information is not used or shared for immigration enforcement purposes, agencies should incorporate safeguards that limit access to and sharing of information in law enforcement databases with internal and external entities. These policies and procedures should contain:
    - The legal authorities that authorize or prohibit the sharing of the personal information with internal and external entities. For example, the Values Act prohibits agencies from providing personal information about an individual, including but not limited to an individual's home or work addresses, for immigration enforcement purposes, unless that information is available to the public. *See* Cal. Gov't Code § 7284.6(a)(1)(D).
    - A definition of "immigration enforcement" that is consistent with the Values Act; and a definition of what would permissible non-"immigration enforcement" purposes for sharing information. For example, an entity that seeks information about an individual with criminal convictions for purposes of investigation of criminal or civil immigration law violations is seeking information for "immigration enforcement" purposes.
    - A process for the agency to assess and confirm whether the information is being requested for authorized purposes, and not for immigration enforcement purposes.
    - A process for determining whether the purpose for which the information will be used or shared by the recipient is compatible with the purpose for which the information was originally collected. For example, a law enforcement agency that provides a certification for a U visa applicant should not share information about that applicant to other agencies that wish to use that information for any purpose other than investigating the crime that was the subject of the certification.
    - A requirement that the requesting entity certify the purpose for which it seeks the information, and that the information will not be used for immigration enforcement purposes.
    - A requirement that the requesting entity certify that it will protect the personal information from further dissemination beyond the requesting entity.

- While the California Values Act does not prohibit or restrict law enforcement agencies from sharing information about an individual's immigration or citizenship status, agencies may adopt generally-applicable privacy policies that restrict the collection, use, and dissemination of any and all personal information.[6]

- Agencies should refrain from providing agencies involved in immigration enforcement with direct access to their databases, law enforcement or otherwise. Information should be shared through a method by which the agency holding the personal information is able to evaluate each request independently according to the applicable law, policies, and procedures.

- If direct access is provided to law enforcement agency databases, the databases should be configured so that different types of users are provided access only to information that they have a right to know, need to know, and are authorized to receive under the California Values Act.

[6] *See City of New York v. United States*, 179 F.3d 29, 36-37 (2d Cir. 1999).

- Agencies should share personal information from law enforcement agency databases on an individualized basis and should avoid blanket, ongoing, or mass sharing of personal information from databases. Sharing of personal information on an individualized basis allows agencies the opportunity to obtain certification from the requesting agency of the purpose for each inquiry, thereby allowing the agencies to subsequently audit the use and disclosure of that data.

- Agencies should notify the individuals whose personal information they are sharing with requesting agencies, where that notification is not otherwise prohibited by law. The notice should contain the information being shared, along with whom it is being shared, so that the individual may contest the accuracy of that information, or update or amend that information.

- Agencies should be aware that, even if they do not share personal information directly with an agency for purposes of immigration enforcement, they may share personal information with other local, state, out-of-state or federal agencies, contractors or vendors, or other private companies offering data services. Agencies should ensure, by contractual terms, certifications, or other written agreements, that those recipients do not further share personal information in a manner that would allow it to be used for immigration enforcement purposes.

Accountability and Auditing, and Transparency

- Agencies that collect personal information that may be used for immigration enforcement purposes should implement appropriate security, auditing, and accountability measures to ensure that this information is handled appropriately.

- Agencies should conduct regular audits of the access, queries, and disclosure of personal information from their law enforcement databases to internal and external entities. Agencies should ensure that they collect sufficient information from the requestors about their purposes in order to assess whether the sharing of information was lawful, authorized, and compatible with the agency's privacy policy.

- Agencies should adopt retention policies to ensure that personal information contained in law enforcement databases relating to place of birth, employment or other personal information that may be used for immigration enforcement purposes are retained for the period necessary to fulfill the purposes for which it was initially collected and no longer.

- Agencies should adopt training requirements for their employees and contractors on the applicable laws and policies to ensure that the collection of personal information comports with these frameworks. Further, employees and contractors of the agencies should be instructed that they are not to allowed to share personal information in databases with federal agency personnel engaged in immigration enforcement, except as authorized and permitted under California law.

- The agency should periodically and publicly disclose how many requests it received from immigration authorities, the legal justifications underlying those requests (e.g., 50 warrants received in 2018, 250 administrative subpoenas, etc.), how it responded to those requests (i.e., percentage of requests complied with), the categories of personal information it provided in

response to those requests, the number of Californians that were the subject of those requests, and whether notice was provided to the subjects of those requests.

- Agencies should publish a privacy policy setting forth, for each database operated by the agency:

    - **Collection of Personal Information:** the categories of personal information their databases hold; and the legal authority to collect each category of personal information;
    - **Purpose and Authorized Uses:** the purposes and use for which each piece of personal information is authorized; any future purposes or the circumstances under which such information may be shared; any justification necessary to share the information; the compatibility between intended uses or sharing of that information and the original purposes for which the information was retained;
    - **Data Access:** the individuals who can access or use the personal information; the rules and processes required to such access;
    - **Data Protection:** the safeguards that protect information from unauthorized access including encryption and access control mechanisms;
    - **Data Retention:** the time period, if any, for which personal information will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.
    - **Public Access:** how collected information can be accessed or used by members of the public, including criminal defendants.
    - **Third Party Data Sharing**: a description of the sharing of personal information that is authorized and permitted; the legal authorities governing the sharing of personal information, including any required justification or legal standard necessary to do so; the categories of internal and external entities with which it shares personal information; any obligations imposed on the recipient of the information; and any notification procedures for individuals whose personal information is being shared.
    - **Training:** the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials
    - **Auditing and Oversight:** any mechanisms to ensure that the privacy policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, and any independent person or entity with oversight authority.

- To further transparency and accountability regarding access to databases throughout the state, the Attorney General's office should inquire of state, county, and local agencies whether they directly or indirectly provide DHS, ICE, or CBP access to personal information in their possession.

V. Recommendations for Specific Databases and Data-Sharing Arrangements in California

In addition to recommendations for generally-applicable guidelines for law enforcement databases, below are recommendations specific to certain databases and data-sharing arrangements in California that may involve personal information being shared for immigration enforcement purposes.

Databases Holding Personal Information Collected and Maintained by the California Department of Motor Vehicles

The California Department of Motor Vehicles ("DMV") contains records relating to drivers' licenses issued to residents of California, including drivers' licenses issued under AB 60. The DMV databases hold personal information regarding drivers, including addresses, physical descriptions, drivers' license photographs, vehicle registration information, and license plate numbers. Currently, approximately 40 agencies of DHS, including Customs and Border Protection and Immigration and Customs Enforcement, are authorized to request information from DMV databases. These agencies may request information as Government Requesters by online means, by telephone, or using a state government form; online through the California Law Enforcement Telecommunications System (CLETS); through the CalPhoto database; and through the national criminal justice information exchange system Nlets. Since 2013, DHS and its agencies have made hundreds of inquiries each year to obtain information contained in the DMV databases. To ensure that information in held by DMV is not shared for immigration enforcement purposes, we recommend:

- DMV and the California Department of Justice ("DOJ") should clearly disclose the various mechanisms by which DHS and component agencies may obtain driver's license and vehicle registration information and what information is provided through each mechanism.

- DMV and CA DOJ should establish standards and policies for the initial assessment and periodic re-assessment of external agencies' requests for government requestor accounts or authorization to access information held in DMV databases.

- DMV and CA DOJ should create a process for determining whether an external agency seeking access to personal information in DMV databases is doing so for immigration enforcement purposes or another lawful purpose. Authorized purposes for accessing DMV information should not include immigration enforcement.

- DMV and CA DOJ should require agencies that seek information in DMV databases through CLETS, Nlets, government requestor accounts, or similar mechanisms to provide sufficient information to demonstrate the basis for each inquiry and how the information is in furtherance of an authorized purpose and not immigration enforcement purposes. Merely providing a case number or docket number related to an inquiry is insufficient.

- DMV should keep copies of any requests by DHS or its components for driver's license or vehicle registration information by any method of access. DMV should keep copies of its responses to any such requests.

- DMV should notify individuals when DMV or CA DOJ provides personal information to DHS agencies, such as individual's driver's license, vehicle registration, or address information.

- Access to the DMV databases through CLETS, government requestor accounts, Nlets or any other means should be logged, record, and audited. The audits should include the agencies and individuals making queries, the actual queries, the responses to the queries, the number of queries, the basis for queries, and any violations of conditions of access or the rules governing use of information obtained through these systems. The audits should be made public.

- A judicial warrant or court order should be required for access to documents furnished by an individual to DMV to provide identity or residency. DMV should not disclose such records in response to an administrative subpoena absent a court order enforcing the subpoena. To the extent records are disclosed in response to an administrative subpoena, DMV should provide notice to the individual who is the subject of the subpoena, as required by California Civil Code § 1798.24(k).

- Plans for sharing of information through a state-to-state verification system pursuant to the Real ID Act or otherwise should be publicly disclosed. Stakeholders should be involved in any discussions regarding the manner in which California will participate in the system. Limits regarding the kind of information that will be shared and stored through the system should also be imposed. Any sharing should protect the confidentiality of information or documents provided by driver's license applicants, including documents used to establish identity or residency, or documents or information that could reveal a person's country of birth, social security number or lack of SSN, citizenship or immigration status, or other sensitive information.

Fusion Centers Comprising Federal, State, and Local Agencies

There are four fusion centers in California, which are state-funded entities that disseminate information between state and federal actors. Originally formed for counterterrorism ends, fusion centers today collect and aggregate significant amounts of information not related to terrorism or serious crimes.[7] For example, a fusion center in Northern California, the Northern California Regional Intelligence Center, amasses significant information from law enforcement agencies in the region, including social media data, information about California drivers collected by automated license plate readers, and "suspicious activity reports" submitted by law enforcement agencies.[8] Despite Congressional findings that fusion centers pose serious privacy risks with little benefit to public safety,

[7] Faiza Patel, Michael Price, *Fusion Centers Need More Rules, Oversight*, Brennan Center, Oct. 18, 2012, https://www.brennancenter.org/analysis/fusion-centers-need-more-rules-oversight.
[8] Matt Cagle, *Use of Automated License Plate Readers Expanding in Northern California, and Data is Shared With Feds*, ACLU Free Future blog, July 22, 2013, https://www.aclu.org/blog/national-security/use-automated-license-plate-readers-expanding-northern-california-and-data;

California law enforcement agencies continue to share Californians' data with federal immigration authorities that request and access that personal information.[9]

- ➢ Fusion centers should adopt the general-applicable guidelines outlined in Section IV above. These guidelines ensure that personal information that may be later used for immigration enforcement purposes is not needlessly collected; that any access to or sharing of personal information provided to federal agencies is not for the purposes of immigration enforcement; and that any access to their databases by state and federal officials is logged and independently audited.

- ➢ Fusion centers should be required to adopt strict retention limits for any information they collect and maintain. Fusion centers should delete information collected from California agencies by the fusion center's own retention deadline, or the originating local agency's retention schedule, whichever is shorter.

- ➢ Fusion centers should adopt privacy policies that includes the information described at Section IV above. These privacy policies should address the different surveillance databases operated by a fusion center, describe any databases accessible to federal authorities and the categories of information contained in those databases, and any legal justification necessary for federal law enforcement to access information in those databases.

- ➢ The Attorney General should recommend the following for California law enforcement agencies regarding their interactions with fusion centers.
    - o California agencies should be instructed not to share personal information with fusion centers unless that information is related to a criminal investigation.[10] Regardless of the justification for sharing information, California agencies should not submit any information to a fusion center from which immigration status could be derived.
    - o California agencies should be prohibited from accessing fusion center databases unless the agency justifies its access based on an active criminal investigation.

Databases Holding Information Collected by Surveillance Technology

Many California law enforcement agencies – including police departments, sheriffs, and district attorneys – operate and maintain large databases filled with information collected by surveillance technologies.[11] Federal immigration authorities may seek to exploit these local databases for

---

[9] *Investigative Report Criticizes Counterterrorism Reporting, Waste at State & Local Intelligence Fusion Centers*, Permanent Subcommittee on Investigations, U.S. Senate Committee on Homeland Security & Governmental Affairs, Oct. 3, 2012, https://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

[10] 28 C.F.R. Part 23 requires reasonable suspicion of criminal activity, which should be adopted as the standard federal agencies must meet in order for California agencies to share information from databases.

[11] "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology includes, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition

immigration enforcement purposes. This concern is not theoretical – earlier this year, media reports detailed how ICE had purchased access to a nationwide database of location information about California drivers.[12] Many California law enforcement agencies operate license plate readers that collect this very information.[13]

- ➢ Law enforcement agencies operating surveillance technology databases should adopt privacy and use policies ("surveillance use policies") for each local database containing information collected with a surveillance technology. The surveillance use policies should include the information described at Section IV of this document.

- ➢ Surveillance use policies adopted by law enforcement agencies should first receive approval by local governing bodies, which should make a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the governing body's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

California Law Enforcement Telecommunications System ("CLETS")

The California Law Enforcement Telecommunications System ("CLETS") is a communications network that is overseen by the California Department of Justice. Through CLETS, participating law enforcement agencies, which include DHS and its component agencies, may make electronic inquiries regarding an individuals' criminal history, as well as other records including Department of Motor Vehicle records. Under the Values Act, California law enforcement may respond to a request from immigration authorities for information about a "specific person's criminal history, including previous criminal arrests, convictions, or similar criminal history information accessed through [CLETS]." Cal. Gov't Code § 7284.6(b)(2). The Values Act, thus, limits the information sharing to a narrow sort of information and is clear that the sharing must be individualized. We further recommend the following guidelines be adopted to avoid CLETS being used for purposes of immigration enforcement:

- ➢ CADOJ should create tiers for different levels of access to CLETS and the information available through CLETS. The level of access granted to a CLETS user should depend on the nature of the user and the purpose of their use of CLETS, with California entities receiving one form of access, out-of-state and federal agencies another form of access, and agencies engaged in immigration enforcement a limited form of access.

- ➢ The Policies, Procedures, and Practices (PPPs) for CLETS should contain directions on the steps that law enforcement agencies must undertake to ensure their own terminals/CLETS systems are not accessed by federal agency personnel engaged in immigration enforcement.

---

software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

[12] Russell Brandom, *Exclusive: ICE is about to start tracking license plates across the US*, The Verge, Jan. 26, 2018, https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions.

[13] *See* State of Surveillance: Automated License Plate Readers, ACLU of Northern California, https://www.aclunc.org/article/map-state-surveillance-california#tab2.

- ➢ Mandatory CLETS training must include instructions to law enforcement agency officers that they are not to allowed to share CLETS information with federal agency personnel engaged in immigration enforcement, except as allowed under law.

- ➢ CADOJ should affirmatively investigate allegations of misuses of CLETS by any CLETS user, including federal agencies. CADOJ should not rely upon CLETS user agencies to investigate their own misuse.

Gang Databases

Databases used to record suspicions of gang membership or association are a source of particular concern because of the low threshold for making gang allegations and the dramatic effect these allegations have in the immigration context. California law enforcement agencies maintain three categories of gang databases. The first category is the registry of individuals convicted of a gang crime. This registry is mandated by the California Penal Code §§ 186.30-186.33.

The second category consists of shared databases of individuals that law enforcement agencies merely suspect of gang membership or association, or have defaulted or been adjudicated gang members under a lesser standard than required for criminal conviction. California Penal Code §§ 186.34-186.36 govern the use of these shared gang databases. Suspicion of gang membership is typically based on innocent activity such as wearing sports gear or associating with friends. CalGang is the largest database in this category and houses data on individuals perceived to be members of street gangs, including physical descriptions, tattoos, associates, locations, vehicles, field interviews, criminal histories and activities. The database is overseen by the California Department of Justice. [14] The California State Auditor published a report in August 2016 revealing various flaws with CalGang, including but not limited to, failing to protect privacy rights, lack of reasonable suspicion for placing groups onto the database, and a lack of governmental oversight or public transparency.[15]

The third category consists of local gang databases that are comprised of some or all of the above information, but are kept "in-house" by law enforcement agencies, and to which other agencies do not have direct access. Because these databases are not shared, they are not subject to the laws or regulations cited above that govern shared gang databases. However, these databases are within the scope of and covered by the California Values Act.

In addition to these three categories, several jurisdictions in California maintain databases of "enforcement lists" for gang injunctions. These databases consist of lists of individuals that prosecutors believe are gang members and therefore subject to civil injunctions against the gang. Historically, nearly all people on enforcement lists were included without any judicial process.

We recommend the following guidelines to ensure that the gang databases are not used for purposes of immigration enforcement:

---

[14] *See* What is CalGang, State of California Department of Justice, https://oag.ca.gov/calgang.

[15] Elaine M. Howell, The CalGang Criminal Intelligence System Report 2015-130, California State Auditor, Aug. 2016, https://www.auditor.ca.gov/pdfs/reports/2015-130.pdf

- Regulations currently being drafted separately by the CA DOJ's CalGang Unit regarding shared gang databases should be consistent with the recommendations in Section IV, supra, in order to ensure the use of shared gang database for immigration enforcement purposes is limited to the maximum extent possible.

- CA DOJ should issue a bulletin instructing jurisdictions to update their Field Interview (FI) cards.[16] The bulletin shall instruct jurisdictions to terminate use of any FI cards that reference or prompt an officer to inquire into an individual's social security number, nationality, country of origin, or immigration status, and provide officers with new FI cards that are compliant with the California Values Act.

- CA DOJ shall ensure that the personally-identifiable information, including but not limited to, physical descriptions, home or work addresses, telephone numbers, and date of birth, contained in a Field Interview card that is uploaded into a database such as CalGang or any other criminal DOJ-operated criminal history systems, is not made available to federal immigration authorities.

- Law enforcement agencies shall keep all written requests and documentation filed by individuals, parents or guardians, and attorneys under AB 2298 (Weber) private and inaccessible to federal immigration authorities.[17]

- If information from any category of gang databases or enforcement lists are shared with federal agencies for non-immigration purposes, law enforcement agencies should clearly distinguish between: (1) individuals who have been found to be gang members in judicial proceedings such as those described in Penal Code § § 186.30-186.33 or who have been found to be gang members after a hearing in a gang injunction case; (2) individuals who have defaulted or been adjudicated gang members outside of the criminal context; and (3) individuals merely suspected of gang membership.

- Because of the risk of immigration enforcement as a collateral consequence of federal criminal investigations, identities of those suspected of gang membership may be shared with federal agencies only for criminal investigations into specific crimes reasonably suspected of having been committed by that individual. If federal agencies purport to investigate crimes reasonably suspected of having been committed under a conspiracy involving that gang's members or an

[16] Currently, some jurisdictions utilize FI's that explicitly ask for social security numbers in direct violation of the California Values Act. Cal. Gov't Code § 7284.6(a)(1)(D).

[17] AB 2298 requires local law enforcement agencies to provide written notice to individuals if they are placed on a shared gang database as an alleged gang member and the basis for the designation. It permits adults to submit written documentation to the local law enforcement agency to contest the allegation. Disclosure of these documents to federal immigration authorities could be harmful to individuals, especially if the challenge to inclusion in the database is denied.

unidentified member of the gang, the identities of those suspected of membership in that gang may be shared. Evidence on which suspicions of gang membership are based, which are not related to the underlying crime being investigated, should not be shared with the investigating federal agency.

- Because of the risk of extra-judicial killings of deported alleged gang members in their home countries, neither suspicions of gang membership nor the evidence on which those suspicions are based should ever be shared with agencies outside the United States.