Bloomberg Law®

Domestic Privacy Profile: California

Prepared in cooperation with

W. Reece Hirsch

Co-head, Privacy & Cybersecurity Practice
Morgan, Lewis & Bockius LLP

Bloomberg Law | Privacy & Data Security

Domestic Privacy Profile: CALIFORNIA

W. Reece Hirsch, co-head of the Privacy & Cybersecurity Practice of Morgan, Lewis & Bockius LLP, San Francisco, provided expert review of the California Profile and wrote the Risk Environment section, with the assistance of San Francisco associate Ellie Chapman. [Last updated October 2017. — Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS 3
A. Constitutional Provisions 3
B. Personal Data Protection Provisions 4
1. Who is covered? 4
2. What is covered? 4
3. Who must comply? 4
C. Data Management Provisions 4
1. Notice & Consent 4
2. Collection & Use 5
3. Disclosure to Third Parties 5
4. Data Storage 6
5. Access & Correction 6
6. Data Security 6
7. Data Disposal 6
8. Data Breach 6
9. Data Transfer & Cloud Computing 7
10. Other Provisions 7
D. Specific Types of Data 7
1. Biometric Data 7
2. Consumer Data 7
3. Credit Card Data 8
4. Credit Reports 8
5. Criminal Records 9
6. Drivers' Licenses/Motor Vehicle Records 9
7. Electronic Communications/Social Media Accounts 9
8. Financial Information 10
9. Health Data 10
10. Social Security Numbers 10
11. Usernames & Passwords 11
12. Information about Minors 11
13. Other Personal Data 11

E. Sector-Specific Provisions 11
1. Advertising & Marketing 11
2. Education 12
3. Electronic Commerce 12
4. Financial Services 12
5. Healthcare 13
6. HR & Employment 13
7. Insurance 14
8. Retail & Consumer Products 15
9. Social Media 15
10. Tech & Telecom 15
11. Other Sectors 15
F. Electronic Surveillance 16
G. Private Causes of Action 16
1. Consumer Protection 16
2. Identity Theft 17
3. Invasion of Privacy 17
4. Other Causes of Action 17
H. Criminal Liability 17
II. REGULATORY AUTHORITIES AND ENFORCEMENT 18
A. Attorney General 18
B. Other Regulators 18
C. Sanctions & Fines 18
D. Representative Enforcement Actions 18
E. State Resources 19
III. RISK ENVIRONMENT 19
IV. EMERGING ISSUES AND OUTLOOK 20
A. Recent Legislation 20
1. Workplace Privacy 20
B. Proposed Legislation 20
1. Security of Connected Devices 20
2. Broadband Privacy 21
3. Invasion of Privacy 21
4. California Cybersecurity Integration Center 21
5. Electronic Communications 21
C. Other Issues 21
1. Data Breach Report 21
2. Ballot Initiative 22

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

Article 1, § 1 of the California Constitution protects the “inalienable rights” of all people, which specifically include privacy.

B. PERSONAL DATA PROTECTION PROVISIONS

Cal. Civ. Code Title 1.8 is the state's overarching personal data regime. Chapter 1 of that title (Cal. Civ. Code §§ 1798 -1798.78), also known as the Information Practices Act of 1977, places limits on the collection, management, and dissemination of personal information by state agencies.

The Civil Code provisions that follow impose requirements on private business entities that have possession of personal data about California residents. For example, Title 1.81 (the Reasonable Security provisions) requires businesses that own, license, or maintain personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure" (Cal. Civ. Code § 1798.81.5(b)).

1. Who is covered?

The Information Practices Act applies to state agencies that maintain information "that identifies or describes an *individual*." Cal. Civ. Code § 1798.3(a) (emphasis added). The term "individual" means a "natural person," Cal. Civ. Code § 1798.3(d), and the term "person" means "any natural person, corporation, partnership, limited liability company, firm, or association," (Cal. Civ. Code § 1798.3(f)).

The Reasonable Security provisions apply to "businesses that own, license, or maintain personal information about *Californians*." Cal. Civ. Code § 1798.81.5(a) (emphasis added). The term "Californians" is not defined, but other provisions of the statute use the term "California resident" (see, e.g., Cal. Civ. Code § 1798.81.5(b)).

2. What is covered?

Under the Information Practices Act, personal information is any information maintained by a state agency that identifies or describes an individual, including, but not limited to, name, Social Security number, physical description, home address, home phone number, education, financial matters, and medical or employment history, including statements made by, or attributed to, the individual (Cal. Civ. Code § 1798.3(a)).

Under the Reasonable Security provisions (Cal. Civ. Code § 1798.81.5), personal information is (1) an unencrypted or unredacted record that contains an individual's first name or initial, last name, and at least one of the following: Social Security number; driver's license or California ID card number; the number of an account or a debit or credit card, in combination with any security code required for access to an account; medical information; or health insurance information; or (2) a username or e-mail address in combination with a password that would permit access to an online account. Personal information does not include information that is lawfully available to the public.

3. Who must comply?

Virtually all California government agencies must comply with the Information Practices Act. Exceptions apply for the state legislature, agencies established under Article VI of the California Constitution (related to the judicial branch), the State Compensation Insurance Fund (except for records containing personal information of employees of the fund), and local agencies as defined under Cal. Gov't Code § 6252(a) (Cal. Civ. Code § 1798.3(b)).

Businesses that "own, license, or maintain personal information about Californians" must comply with the Reasonable Security provisions (Cal. Civ. Code § 1798.81.5(a)). A "business" is defined as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution" (Cal. Civ. Code § 1798.80(a)).

C. DATA MANAGEMENT PROVISIONS

1. Notice & Consent

Various provisions of California law govern individuals' rights to notice and consent regarding their personal information. For example, under the Credit Card Full Disclosure Act, credit card issuers must

provide their customers with a written notice of their right to prohibit the disclosure of marketing information by the issuer that discloses the customers' identities (Cal. Civ. Code § 1748.12(b)).

In addition, businesses or government agencies owning or licensing unencrypted computerized data containing personal information must notify any California resident whose personal information was, or was reasonably believed to have been, acquired by an unauthorized person (Cal. Civ. Code §§ 1798.29, 1798.82; see I.C.8.).

Under the California Financial Information Privacy Act, financial institutions must obtain the consent of the consumer prior to disclosing any nonpublic personal information and must obtain such consent through use of a form, statement, or writing that provides notice to the consumer that by signing, the consumer is consenting to the disclosure and that such consent will remain in effect until revoked or modified (Cal. Fin. Code § 4053).

Finally, under the Insurance Information and Privacy Protection Act, insurers are required to provide a notice to all applicants and policy holders that specifies what information can be collected and any permissible disclosures (Cal. Ins. Code § 791.04).

2. Collection & Use

The Information Practices Act of 1977 governs requirements of state agencies regarding the collection and use of personal information. To the greatest extent practicable, state agencies must collect personal information directly from the individual who is the subject of the information rather than from another source (Cal. Civ. Code § 1798.15). Whatever the source of the information collected, state agencies must maintain the source of the information as specified by law (Cal. Civ. Code § 1798.16).

3. Disclosure to Third Parties

Articles 6 and 7 of the Information Practices Act of 1977 govern the conditions under which personal information may be disclosed by state agencies as well as the accounting steps agencies are required to undertake whenever making such a disclosure (Cal. Civ. Code §§ 1798.24 -1798.24b, 1798.25 - 1798.29).

Cal. Civ. Code § 1798.83, also known as the "Shine the Light" law, requires businesses that have disclosed the personal information of their customers for direct marketing purposes to provide such customers upon request either (a) a list of the categories of personal information the business disclosed and the addresses of the parties to whom the information was disclosed, or (b) a privacy statement giving the customer the right to opt out of any such information sharing.

Cal. Civ. Code § 1748.12 allows credit card holders to prohibit a credit card company from disclosing marketing information to third parties.

Cal. Civ. Code §§ 1799.1 -1799.3 regulate business disclosures, prohibiting disclosure of records by bookkeeping services (Cal. Civ. Code § 1799.1), information relating to a tax return (Cal. Civ. Code § 1799.1a), and video recording sale or rental services records (Cal. Civ. Code § 1799.3).

Under the California Consumer Credit Reporting Agencies Act, such agencies may disclose public record information lawfully obtained by or for the agency from an open public record to the extent permitted by law (Cal. Civ. Code § 1785.11.2(n)).

Cal. Civ. Code § 1798.98 prohibits the disclosure of customer usage data collected by electric and natural gas utilities available to third parties without the express consent of the customer, and requires utilities that disclose such information with customer consent to maintain reasonable security measures to protect the information from unauthorized access, disclosure, modification, or destruction.

Cal. Pub. Util. Code § 2891 prohibits any telephone or telegraph corporation from disclosing a subscriber's personal calling patterns, credit or other personal financial information, or other specified personal information without the written consent of the subscriber, with certain exceptions such as disclosures for debt collection purposes or for responding to 911 calls.

Under the Reader Privacy Act, a business operating as a "book service" (i.e., providing the rental, purchase, borrowing, browsing, or perusal of books) may not disclose personal information concerning a user to any governmental or private entity without a court order or the user's affirmative consent (Cal. Civ. Code § 1798.90).

4. Data Storage

California does not have any general laws governing the storage of personal data by businesses. However, several laws applicable to specific sectors, such as financial institutions, utilities, and other businesses, require them to take steps to ensure the security of personal data in their possession. The California Office of Privacy Protection's Business Privacy Handbook recommends specifically that businesses store paper records containing sensitive personal information in locked cabinets and encrypt electronically stored data containing such information, including data on laptops and other portable devices.

5. Access & Correction

Article 8 of the Information Practices Act of 1977 governs the conditions under which an individual may obtain access to any personal information about him or her in the possession of a state agency. The law specifies the circumstances under which an individual may request correction of inaccurate information, as well as reviews of an agency's refusal to correct and circumstances under which the agency is not required to provide access to an individual (Cal. Civ. Code §§ 1798.30 -1798.44).

Cal. Bus. & Prof. Code §§ 22580 -22582 allow minors to request the removal of personal information on a website and prohibit websites from targeting minors in ads for goods that minors cannot legally buy.

6. Data Security

Cal. Civ. Code § 1798.81.5 requires businesses that own, license, or maintain personal information to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

7. Data Disposal

Cal. Civ. Code § 1798.81 requires a business to take reasonable steps to dispose or arrange for the disposal of customer records within its custody or control containing personal information by shredding, erasing, or otherwise modifying the personal information to make it unreadable or undecipherable through any means.

8. Data Breach

Cal. Civ. Code § 1798.82 requires an entity conducting business in California to disclose a security breach to any California resident that includes either unencrypted information or encrypted information in combination with an encryption key or security credential that could render the information readable or usable. Such notification must be made in the most expedient time possible and without unreasonable delay and must be consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach or restore the data system's integrity.

California's security breach notification law includes one of the more comprehensive definitions of personal information. "Personal information" is defined as (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements: (a) Social Security number; (b) driver's license number or California ID card number; (c) account number, credit or debit card number, in combination with any required security access code, or password that would permit access to an individual's account; (d) medical information, (e) health insurance information; and (f) information or data collected through the use or operation of an automated license plate recognition system; or (2) a username or e-mail address, in combination with a password or security question and answer that would permit access to an online account (Cal. Civ. Code § 1798.82(h)).

The California breach notification law is also unique in that it requires that, if (1) the person or business was the source of the breach, and (2) the breach involved Social Security numbers, driver's license numbers or California ID care numbers, then the notification letter must include an offer to provide appropriate identity theft prevention and mitigation services at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer (Cal. Civ. Code § 1798.82(d)(2)).

9. Data Transfer & Cloud Computing

California law does not contain general provisions regarding data transfers or cloud computing. However, in the education sector, a pair of recently enacted laws address the collection of personal information via students' social media, as well as the increasing reliance by schools on third-party vendors that maintain online sites used to store personal information—including test scores, demographic information, and attendance records, often on the cloud—where it may be vulnerable to hacking or other unintended disclosure.

Cal. Educ. Code § 49073.6 sets forth requirements that schools must meet prior to gathering information via social media on students, including giving parents notice, and provides that information must be deleted if it is no longer being used for a legitimate education purpose, if the student turns 18 or requests deletion, or if the student is no longer a student in the school district, generally within one year.

If a school uses a third-party vendor to gather such information, the contract with the vendor must prohibit it from using the information for anything other than the purposes of the contract or from disclosing the information to anyone other than the school, the pupil, or the pupil's parents. In addition, the vendor must destroy all information immediately upon satisfying the terms of the contract.

Cal. Bus. & Prof. Code § 22584 prohibits operators of online websites or services used primarily for primary and secondary education purposes from using, sharing, compiling, disclosing, or selling personal information about a student except for the school purpose for which the information was collected. The operator must maintain reasonable security procedures, and information must be deleted on request of the school or school district.

10. Other Provisions

Our research has revealed no other generally applicable data management provisions in California.

D. SPECIFIC TYPES OF DATA

1. Biometric Data

Cal. Ins. Code §§ 10140 -10149.1 restrict insurance companies' use of genetic tests and require consent before testing. They prohibit disclosure of genetic tests to third parties. Healthcare service plans are subject to similar restrictions under Cal. Civ. Code § 56.17.

Cal. Civ. Code § 52.7 prohibits a person from requiring another individual to undergo the subcutaneous implanting of an identification device.

Cal. Lab. Code § 1051 permits California employers to collect photographs or fingerprints from employees as a condition of employment, but prohibits employers from sharing this information with another employer or third party. Violations of this provision constitute a misdemeanor.

Cal. Gov't Code § 12940(o) makes it illegal for employers to subject any employee, applicant, or other person to a test for the presence of a genetic characteristic.

Biometric data is considered "covered information" under Cal. Bus. & Prof. Code § 22584, which prohibits operators of online websites or services used primarily for primary and secondary education purposes from using, sharing, compiling, disclosing, or selling covered information about a student except for the school purpose for which the information was collected.

2. Consumer Data

Title 1.81 of the California Civil Code (§§ 1798.80 -1798.84, referred to as the Customer Records provisions) requires that businesses dispose of customer data, disclose security breaches, list categories of information disclosed to third parties or allow consumers to opt out of such disclosure, and remove, upon request, personal information from company websites. Cal. Civ. Code § 1798.84 provides that a customer injured by a violation of the Customer Records title may institute a civil action to recover damages and attorney fees, including injunctive relief as appropriate. Such a customer also may recover a civil penalty of up to $3,000 per violation if the violation is willful, intentional, or reckless, and up to $500 per violation for all other violations.

The Investigative Consumer Reporting Agencies Act (Cal. Civ. Code §§ 1786 -1786.60) regulates investigative consumer reporting agencies. The law restricts collection and disclosure of personal information and provides subjects the right to request data maintained about them.

Cal. Civ. Code § 1798.98 prohibits a business from sharing customer electrical or natural gas data with a third party without the customer's consent. Cal. Pub. Util. Code §§ 8380-8381 provide similar protections for data related to advanced metering infrastructure.

Cal. Civ. Code §§ 1749.64 -1749.65 prohibit supermarket club card issuers from requesting an applicant's driver's license number or Social Security number and prohibit them from selling cardholders' personal identification information.

Cal. Civ. Code §§ 1799.1 -1799.3 regulate business disclosures, prohibiting disclosure of records by bookkeeping services (Cal. Civ. Code § 1799.1), information relating to a tax return (Cal. Civ. Code § 1799.1a), and video recording sale or rental services records (Cal. Civ. Code § 1799.3).

Cal. Civ. Code §§ 1798.90 et seq., also known as the Reader Privacy Act, prohibits commercial entities offering book rental, purchase, or borrowing services from disclosing the personal information of users to third parties.

3. Credit Card Data

Cal. Civ. Code § 1748.12 allows credit card holders to prohibit a credit card company from disclosing marketing information to third parties.

Cal. Civ. Code § 1747.06 requires a credit card issuer that receives an application for a card that lists an address different from the address on the offer or solicitation to verify the change of address by contacting the person to whom the solicitation was mailed. Similarly, Cal. Civ. Code § 1799.1b provides that a credit card issuer that receives a change of address request and, within 60 days of such receipt, receives a request for a new credit card must notify the consumer at the former address of record.

Cal. Civ. Code § 1747.08 prohibits any person, firm, partnership, association, or corporation that accepts a credit card for payment in a transaction from collecting and recording the cardholder's personal information. Exceptions apply, including for collection of zip code information at a gas pump or automated cashier at a gas station, provided that the use of zip code information is limited to fraud prevention.

Cal. Civ. Code § 1747.09 provides that a person, firm, partnership, association, corporation, or limited liability company accepting credit or debit cards for payment in a transaction may print no more than the last five digits of the cardholder's account number, or the card expiration date, on an electronically printed receipt.

Cal. Civ. Code § 1747.05(b) requires credit card issuers to provide an activation process whenever sending a substitute card to a cardholder that mandates that the cardholder contact the issuer to activate the card prior to its first use.

Cal. Penal Code § 502.6 prohibits the knowing and willful possession, with intent to defraud, of "skimmer" devices (tools used to scan or re-encode credit or debit card information using the card's magnetic strip). The law provides for fines and imprisonment for violations, allows the scanning equipment to be seized and destroyed, and permits the forfeiture of any accompanying computer equipment or software used to store illegally obtained data.

4. Credit Reports

The Consumer Credit Reporting Agencies Act, Cal. Civ. Code §§ 1785.1 -1785.36, contains a variety of requirements regarding consumer privacy. Specifically, Cal. Civ. Code § 1785.10 requires agencies to allow consumers to inspect files relating to them (see also Cal. Civ. Code § 1785.15). In addition, under Cal. Civ. Code §§ 1785.11.1 -1785.11.11, agencies must place security alerts on accounts pursuant to a request from a consumer. Finally, agencies must provide consumers with credit scores under specified circumstances (Cal. Civ. Code § 1785.15.1) and must provide a statement to any consumer who has reason to believe that he or she is the victim of identity theft outlining the consumer's statutory rights (Cal. Civ. Code § 1785.15.3).

5. Criminal Records

Under the Investigative Consumer Reporting Agencies Act (Cal. Civ. Code §§ 1786 -1786.60), such agencies may not include in their background report any records of arrest, indictment, information, misdemeanor complaint, or conviction of a crime that, from the date of disposition, release, or parole, took place more than seven years prior to the date of the report (Cal. Civ. Code § 1786.18(a)(7)).

Cal. Penal Code § 432.7 prohibits employers from asking applicants about an arrest or detention that did not result in a conviction or seeking such information from any other source. However, if an applicant is out of jail but awaiting trial, employers may inquire regarding an arrest. In addition, the same restrictions apply to convictions for violations of the California Health and Safety Code related to marijuana possession effective two years from the date of conviction (Cal. Penal Code § 432.8).

Information on convicted sex offenders is available on California's Megan's Law website, but employers may only use such information in an employment decision to the extent that the employer can show that it intends to protect a "person at risk."

Cal. Health & Safety Code § 1598.871 requires a full criminal background check prior to issuing a permit or license to operate a day care facility.

6. Drivers' Licenses/Motor Vehicle Records

Cal. Veh. Code §§ 1800 -1825 requires certain motor vehicle records to be kept confidential, including residence addresses. Section 9951 requires car manufacturers to disclose the fact that a vehicle has an event data recorder installed and restricts retrieval of the data created by such recorders.

Cal. Sts. & High. Code § 31490 protects data belonging to subscribers to electronic toll collection systems and requires agencies that use those systems to inform subscribers of their privacy policies.

Cal. Civ. Code § 1798.90.1 allows businesses to swipe an individual's driver's license or identification card in an electronic device only for the following purposes: age verification or confirmation of the authenticity of the license or card; compliance with a legal requirement to record, retain, or transmit the information; transmission of information to a check service company for payment approvals; or collection or disclosure of personal information required for reporting fraud, abuse, or material misrepresentation.

Cal. Civ. Code § 1939.23 prohibits car rental companies from using, accessing, or obtaining information about a renter obtained using electronic surveillance technology installed in a vehicle.

Cal. Civ. Code §§ 1749.64 -1749.65 prohibit supermarket club card issuers from requesting an applicant's driver's license number or Social Security number and prohibit them from selling cardholders' personal identification information.

7. Electronic Communications/Social Media Accounts

Cal. Lab. Code § 980 prohibits employers from requiring employees to disclose usernames or passwords in association with their social media accounts, requesting that employees access their accounts in the employer's presence, or requesting employees to divulge any personal social media. However, employers may ask employees to divulge information pursuant to an investigation into criminal activity or employee misconduct and may ask for username or password information with respect to an employer-issued electronic device.

Cal. Educ. Code § 49073.6 sets forth requirements that schools must meet prior to gathering information via social media on students, including giving parents notice, and provides that information must be deleted if it is no longer being used for a legitimate education purpose, if the student turns 18 or requests deletion, or if the student is no longer a student in the school district, generally within one year. If a school uses a third-party vendor to gather such information, the contract with the vendor must prohibit it from using the information for anything other than the purposes of the contract or from disclosing the information to anyone other than the school, the pupil, or the pupil's parents. In addition, the vendor must destroy all information immediately upon satisfying the terms of the contract.

The Revised Uniform Fiduciary Access to Digital Assets Act (Cal. Prob. Code §§ 870 -884) allows a person to designate—through a will, trust, power of attorney, or "online tool"—a custodian to disclose

the person's digital assets, including the content of electronic communications (see Cal. Prob. Code § 873).

8. Financial Information

The California Financial Information Privacy Act (Cal. Fin. Code §§ 4050 -4060) governs the responsibilities of financial institutions with respect to nonpublic personal information collected from consumers. In general, such institutions may not sell, share, transfer, or disclose nonpublic personal information to any nonaffiliated third party without explicit prior consent of the consumer (Cal. Fin. Code § 4052.5). For more information, see I.E.4.

Cal. Fin. Code § 4100 prohibits financial institutions from issuing an account number to a customer that was previously used by a different customer for a minimum of three years after the prior account was closed.

Cal. Civ. Code § 1747.09 specifies that no more than the last five digits of a credit or debit card number may be printed on the customer copy of a receipt.

Cal. Civ. Code §§ 1725 and 1747.08 prohibit any person from recording or requiring a credit card number as a condition of accepting a check.

9. Health Data

The California Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56 -56.37) governs disclosures of patient medical information by medical providers, health plans, pharmaceutical concerns, and other businesses organized to maintain medical information. Specifically, providers must obtain authorization prior to disclosing a patient's medical information, unless an exception applies (Cal. Civ. Code §§ 56.10 -56.11). In addition, the Act requires providers, healthcare service plans, pharmaceutical companies, and contractors to maintain medical information in a manner that preserves the confidentiality of personal information and sets forth requirements for electronic health record and medical health record systems (Cal. Civ. Code § 56.101).

Cal. Health & Safety Code §§ 123100 et seq. generally give patients the right to access and copy information maintained by healthcare providers regarding their medical conditions (Cal. Health & Safety Code § 123110). In addition, patients may submit addenda to their health records with respect to any items they find to be incomplete or inaccurate (Cal. Health & Safety Code § 123111).

Cal. Health & Safety Code § 103526 requires that a state or local registrar receiving a request for a certified birth or death certificate accompanied by a notarized statement that the requestor is an authorized person must issue the certificate. However, if the requestor is not an authorized person or does not fulfill the other requirements of the statute, the registrar must issue an informational certified copy bearing the legend "INFORMATIONAL, NOT A VALID DOCUMENT TO ESTABLISH IDENTITY."

Cal. Health & Safety Code § 1280.18 requires healthcare providers to establish and implement administrative, technical, and physical safeguards to protect the privacy of patients' medical information.

Cal. Civ. Code § 1798.91 prohibits businesses from obtaining medical information from an individual for direct marketing purposes, either orally or in writing, unless the business clearly discloses that it is obtaining the information to market or advertise products to the individual and obtains the individual's consent.

Cal. Welf. & Inst. Code § 5328 makes information relating to provision of mental health services confidential and restricts its disclosure.

Cal. Health & Safety Code §§ 120975 -121023 prevent disclosure of information that would identify that an individual has been subject to a test for HIV or AIDS.

Cal. Civ. Code §§ 56.20 -56.245 govern employer obligations with respect to medical information collected from employees. See I.E.6.

10. Social Security Numbers

Cal. Civ. Code §§ 1798.85 -1798.89 prohibit disclosure of a person's Social Security number and recording of a public document displaying more than the last four digits of a Social Security number.

Cal. Lab. Code § 226 provides that, on statements of wages required to be provided to employees, employers, including state and local agencies, may only include the last four digits of the employee's Social Security number, or an employee identification number other than a Social Security number.

Cal. Fam. Code § 2024.5 provides that a petitioner or respondent in a petition for dissolution or nullity of marriage or legal separation may redact Social Security numbers from the petition. However, an abstract of support judgment or other document created for spousal or child support purposes may not be redacted.

11. Usernames & Passwords

Cal. Educ. Code § 99121 prohibits postsecondary educational institutions from requiring students, prospective students, or student groups to disclose social media usernames and passwords.

Cal. Lab. Code § 980 prohibits employers from requiring employees to disclose usernames or passwords in association with their social media accounts, requesting that employees access their accounts in the employer's presence, or requesting employees to divulge any personal social media. However, employers may ask employees to divulge information pursuant to an investigation into criminal activity or employee misconduct and may ask for username or password information with respect to an employer-issued electronic device.

12. Information about Minors

Cal. Bus. & Prof. Code § 22580 prohibits operators of Internet websites, online services, and online and mobile applications from marketing or advertising certain specified products or service to minors living in California. The prohibition applies to all operators who direct their services to minors as well as operators who have actual knowledge that minors are using the sites, services, or applications. Restricted products and services include alcoholic beverages, firearms, guns and ammunition, and tobacco, among other items (see Cal. Bus. & Prof. Code § 22580(i)). Cal. Bus. & Prof. Code § 22581 further provides that operators of such sites, services, or applications must permit users to remove content posted by the user, as well as provide notice of the right to remove content together with clear instructions on how to remove it.

Several provisions of the California Code (primarily the Family Code) allow for minors to consent to medical care without the assistance of an adult guardian. In many instances, healthcare providers must inform the minor's parent or guardian, but depending on the wording of the law at issue, the healthcare provider may not be permitted do so, for example, if the minor provides his or her own consent for the prevention or treatment of pregnancy (except sterilization) or seeks birth control without parental consent. The Adolescent Health Working Group has compiled a toolkit that outlines specific requirements regarding notice and confidentiality requirements when minors exercise their rights to seek medical treatment or care.

13. Other Personal Data

Cal. Gov't Code §§ 6208.1, 6215.10, and 6218 prohibit people and businesses from posting information belonging to certain victims of domestic abuse and certain reproductive healthcare providers, who may also request the removal of personal information from Internet sites. Similarly, Cal. Civ. Code §§ 1798.79.8 -1798.79.95 provide that non-governmental domestic violence victim service providers may not be required to provide personally identifying information concerning current or potential clients as part of an application for grants or other financial assistance.

Cal. Penal Code § 502 makes it a crime to knowingly access and, without permission, alter, damage, destroy, or otherwise use any computer, system, or network for purposes of committing fraud or wrongfully obtaining or controlling money, property, or data. The law provides for imprisonment and fines for violations of its provisions.

E. SECTOR-SPECIFIC PROVISIONS

1. Advertising & Marketing

Cal. Bus. & Prof. Code §§ 17528.41-17538.45 and §§ 17529 et seq. prohibit people or entities from sending unsolicited commercial e-mails or text messages (1) from California e-mail addresses or (2) to

California residents or e-mail addresses. Cal. Bus. & Prof. Code §§ 17590 -17594 prohibit certain calls directed to anyone on the national do-not-call list.

Cal. Civ. Code § 1798.91 prohibits businesses from requesting medical information from an individual or disclosing medical information for direct marketing purposes without receiving informed consent to do so.

Cal. Civ. Code § 1748.12 allows credit card holders to prohibit a credit card company from disclosing marketing information to third parties.

Cal. Bus. & Prof. Code § 22580 prohibits operators of Internet websites, online services, and online and mobile applications from marketing or advertising certain specified products or services to minors living in California. See I.D.12.

Cal. Ins. Code § 791.13(k) provides that insurers may disclose personal information in connection with the marketing of a product or service, but only if the individual has been given the opportunity to "opt out" of any such disclosure for marketing purposes.

Cal. Educ. Code § 89090 permits trustees, alumni associations, and auxiliary organizations affiliated with the California State University system to distribute the names, addresses, and e-mail addresses of alumni to businesses to allow such businesses to provide the alumni with material related to the university, to provide the alumni with commercial opportunities, or to promote the educational mission of the university. To do so, however, a trustee, alumni association, or auxiliary organization must have an agreement with the business in which it maintains control of the data and the business is required to maintain the confidentiality of the information and prohibited from using the information for any other purpose. Additionally, trustees, alumni associations, or auxiliary organizations must inform alumni that the information may be shared and they have the option to "opt out" of the disclosure.

2. Education

Cal. Bus. & Prof. Code § 22584, also known as the Student Online Personal Information Protection Act, prohibits websites designed for K-12 school purposes from using student information to target advertising toward students.

Cal. Educ. Code § 99121 prohibits postsecondary educational institutions from requiring students, prospective students, or student groups to disclose social media usernames and passwords.

Cal. Educ. Code §§ 49073 et seq. govern retention and storage of pupil records and restrict monitoring of student social media.

3. Electronic Commerce

The Online Privacy Protection Act of 2003 (Cal. Bus. & Prof. Code §§ 22575 -22579) requires operators of commercial websites that collect personal information about California residents to conspicuously post or make available a privacy policy and comply with it. The policy must, among other items, specify categories of personally identifiable information collected and the third parties with which the operator may share the information. The Act may be violated by the operator if it fails to comply either (a) knowingly and willfully or (b) negligently and materially, provided, however, that an operator is in violation of the Act only if it fails to post a compliant policy within 30 days after being notified of noncompliance.

Cal. Bus. & Prof. Code §§ 22580 -22582 prohibit websites from targeting minors in ads for goods that minors cannot legally buy. See I.D.12.

4. Financial Services

The California Financial Information Privacy Act (Cal. Fin. Code §§ 4050 -4060) governs financial institutions' handling of personal data and prohibits financial institutions from disclosing a consumer's personal information without his or her consent (Cal. Fin. Code §§ 4052.5 -4053). The law provides that consumers must affirmatively "opt in" before a financial institution may share personal information with an unaffiliated third party (Cal. Fin. Code § 4053(a)). With respect to information sharing with a financial institution's affiliates, the consumer must be provided with notice of such sharing and the opportunity to "opt out" of the sharing, with certain specified exceptions (Cal. Fin. Code § 4053(b)).

5. Healthcare

Cal. Civ. Code §§ 56 -56.37 establish the confidentiality of medical information and govern disclosure by health providers, employers, and third parties. See I.D.9.

Cal. Civ. Code § 1798.91 prohibits businesses from obtaining medical information from an individual for direct marketing purposes, either orally or in writing, unless the business clearly discloses that it is obtaining the information to market or advertise products to the individual and obtains the individual's consent.

Cal. Health & Safety Code §§ 123100 et seq. generally give patients the right to access and copy information maintained by healthcare providers regarding their medical conditions (Cal. Health & Safety Code § 123110). In addition, patients may submit addenda to their health records with respect to any items they find to be incomplete or inaccurate (Cal. Health & Safety Code § 123111).

Cal. Health & Safety Code § 1280.18 requires healthcare providers to establish and implement administrative, technical, and physical safeguards to protect the privacy of patients' medical information.

Cal. Civ. Code § 56.17 provides for civil penalties and fines, as well as liability for a civil cause of action, for any healthcare service plan that willfully or negligently discloses genetic test results to a third party without authorization.

Cal. Civ. Code § 1798.85(e) provides that healthcare service plans, healthcare providers, and other entities involved in the provision or administration of healthcare may not publicly post or display an individual's Social Security number, print an individual's Social Security number on a membership card, require an individual to provide a Social Security number over the Internet unless the connection is secure and the number is encrypted, print a Social Security number on any materials mailed to the individual unless otherwise required by law, or sell an individual's Social Security number.

Cal. Welf. & Inst. Code § 5328 makes information relating to provision of mental health services confidential and restricts its disclosure.

Cal. Health & Safety Code §§ 120975 -121023 prevent disclosure of information that would identify that an individual has been subject to a test for HIV or AIDS.

6. HR & Employment

California employers routinely conduct background checks on job applicants that will include such elements as credit checks, criminal background checks, driving records, and online searches, and also conduct checks of current employees, in particular with respect to misconduct or criminal activity. However, both federal and California laws restrict the scope of such searches to a significant degree. A number of provisions apply, including the following:

- Cal. Lab. Code § 1051 permits California employers to collect photographs or fingerprints from employees as a condition of employment, but prohibits employers from sharing this information with another employer or third party. Violations of this provision constitute a misdemeanor.
- Cal. Gov't Code § 12940(o) makes it illegal for employers to subject any employee, applicant, or other person to a test for the presence of a genetic characteristic.
- Cal. Penal Code § 432.7 prohibits employers from asking applicants about an arrest or detention that did not result in a conviction or seeking such information from any other source. However, if an applicant is out of jail but awaiting trial, employers may inquire regarding an arrest. In addition, the same restrictions apply to convictions for violations of the California Health and Safety Code related to marijuana possession effective two years from the date of conviction (Cal. Health & Safety Code § 432.8).
- Information on convicted sex offenders is available on California's Megan's Law website, but employers may only use such information in an employment decision to the extent that the employer can show that it intends to protect a "person at risk."
- Cal. Health & Safety Code § 1598.871 requires a full criminal background check prior to issuing a permit or license to operate a day care facility.

- Cal. Lab. Code § 980 prohibits employers from requiring employees to disclose usernames or passwords in association with their social media accounts, requesting that employees access their accounts in the employer's presence, or requesting employees to divulge any personal social media. However, employers may ask employees to divulge information pursuant to an investigation into criminal activity or employee misconduct and may ask for username or password information with respect to an employer-issued electronic device.

The Privacy Rights Clearinghouse has compiled an overview of issues related to background checks in California, and a comprehensive Guide for California Nonprofits and Small Businesses on background check provisions is available at the pro bono Public Counsel website.

On July 1, 2017, new regulations enacted by the Fair Employment and Housing Council went into effect that govern employers' rights with respect to using criminal records in employment decisions. The regulations restrict such uses if they have an adverse impact on a prospective or current employee, unless the employer can show that the use is job-related and consistent with business necessity.

Miscellaneous provisions: The provisions of California law governing the duties of businesses to protect personal information (see I.B.), to disclose data breaches (see I.C.8.), and to lawfully conduct electronic surveillance with respect to their employees in accordance with the California Penal Code (see I.F.) apply to employers with respect to the personal information they collect from employees. In addition, the following laws apply:

- Cal. Lab. Code § 435 prohibits employers from recording employees in restrooms, locker rooms, or rooms designated by the employer for changing clothes.

- The California Labor Code further prohibits an employer from considering a polygraph or similar test (Cal. Lab. Code § 432.2) or an expunged, sealed, or dismissed criminal record (Cal. Lab. Code § 432.7) in an employment decision. An employer also may not request disclosure of or access to social media information (Cal. Lab. Code § 980; see I.D.7.).

- Cal. Lab. Code § 226 provides that on statements of wages required to be provided to employees, employers, including state and local agencies, may only include the last four digits of the employee's Social Security number, or an employee identification number other than a Social Security number.

- Cal. Lab. Code § 1198.5 gives current and former employees the right to access and inspect their personnel records and requires employers to maintain such records for at least three years after termination of employment. The law specifies the time and place at which employers must make such records available.

- Cal. Gov't Code § 12940(o) makes it illegal for employers to subject any employee, applicant, or other person to a test for the presence of a genetic characteristic. In addition, while Cal. Gov't Code § 12940(e) prohibits employers from discrimination on the basis of mental or physical disability or medical condition, the law does permit employers to inquire into an applicant's or employee's ability to perform job-related functions and respond to an employee's request for accommodation, and to seek medical or psychological information or require an examination after making an offer to an applicant but prior to commencement of employment if the inquiry or examination is job-related and consistent with business necessity.

- Cal. Civ. Code §§ 56.20 -56.245 govern employer obligations with respect to medical information collected from employees. In general, employers must establish appropriate procedures to protect such information and may not disclose the information without written authorization from the employee. In addition, employers may not discriminate against any employee who refuses to sign an authorization to disclose.

- Cal. Health & Safety Code § 120980(f) specifies that the results of an HIV test may not be used in any instance to determine suitability for employment.

7. Insurance

The Insurance Information and Privacy Protection Act (Cal. Ins. Code §§ 791 -791.29) governs the collection, use, and disclosure of information gathered by insurance institutions, agents, or

organizations. It includes provisions that require insurers to provide notice to applicants and policyholders on their information practices, prohibit disclosure except under specific circumstances, and allow access to information by individuals, as well as processes governing correction, amendment, or deletion. It also outlines the steps health insurers must take to protect the confidentiality of an insured's medical information.

Cal. Ins. Code §§ 10140 -10149.1 restrict insurance companies' use of genetic tests and require consent before testing. They prohibit disclosure of genetic tests to third parties.

Cal. Civ. Code § 56.265 prohibits underwriters or sellers of annuity contracts or insurance against loss, damage, illness, disability, or death from disclosing personal information regarding the health, medical history, or genetic information of a customer to any affiliated or nonaffiliated financial institution or other third party in the business for use with respect to granting credit to the customer.

8. Retail & Consumer Products

Cal. Civ. Code §§ 1749.64 -1749.65 prohibit supermarket club card issuers from requesting an applicant's driver's license number or Social Security number and prohibit them from selling cardholders' personal identification information.

Cal. Civ. Code § 1793.1(a)(1)(B) specifies that with respect to any product warranty card provided to a consumer by a manufacturer, retailer, or distributor of consumer goods, the card must clearly state that the failure to complete and return the card does not diminish the consumer's rights under the warranty.

9. Social Media

Cal. Educ. Code § 99121 prohibits postsecondary educational institutions from requiring students, prospective students, or student groups to disclose social media usernames and passwords.

Cal. Educ. Code § 49073.6 sets forth requirements that schools must meet prior to gathering information via social media on students. See I.C.9.

Cal. Lab. Code § 980 prohibits employers from requiring employees to disclose usernames or passwords in association with their social media accounts, requesting that employees access their accounts in the employer's presence, or requesting employees to divulge any personal social media. However, employers may ask employees to divulge information pursuant to an investigation into criminal activity or employee misconduct and may ask for username or password information with respect to an employer-issued electronic device.

10. Tech & Telecom

Cal. Pub. Util. Code §§ 2891-2891.10 prohibit providers of telecommunications services, including telephone and VoIP providers, from disclosing subscribers' personal information to another person or corporation without written consent. Subscribers may request that their numbers be withheld from the recipient's caller ID at no charge, although such information may not be withheld by businesses using their number for telemarketing purposes.

Cal. Bus. & Prof. Code §§ 22948.20 -22948.25 require television manufacturers to disclose the existence of voice recognition features and prohibit anyone from using or selling recordings for advertising purposes.

Cal. Pub. Util. Code § 2891.1 prohibits a cell phone service provider from listing a subscriber's number in a directory without the subscriber's consent.

Cal. Bus. & Prof. Code §§ 22948.5 -22948.7 require manufacturers of wireless access devices to include a warning that advises consumers how to protect wireless network connections.

Cal. Penal Code § 638 makes it a crime for any person, including a business entity, to purchase, sell, offer to purchase or sell, or conspire to purchase or sell a telephone calling pattern or list without the written consent of the subscriber.

11. Other Sectors

Under Cal. Civ. Code §§ 1798.90.5 -1798.90.55, automated license plate recognition (ALPR) operators must maintain reasonable security features and practices to protect ALPR information from

unauthorized access, use, disclosure, or destruction. The law specifies the required elements of an ALPR's usage and privacy policy and requires operators to maintain a record of all access granted to the information. The law further requires ALPR end-users to whom information is provided to maintain similar security safeguards and to develop a usage and privacy policy.

F. ELECTRONIC SURVEILLANCE

Cal. Penal Code §§ 630 -638.55 penalize invasion of privacy through unlawful tapping, eavesdropping, recording, or opening of telephone communications or telegraphic messages, including communications by radio telephone, cellular radio telephone, cable, or any other device. In addition, cable TV and satellite TV operators are not permitted to monitor or record conversations in a subscriber's home or to share personally identifiable information (such as viewing habits, shopping preferences, medical or banking data, or other information) without the subscriber's express written consent.

Cal. Civ. Code § 1798.79 prohibits any person or entity from intentionally reading or attempting to read another person's identification document (i.e., driver's license, employee ID card, etc.) remotely using radio frequency identification (RFID), unless an exception applies. The provision also prohibits disclosure of the operational system keys used in a contactless identification document system. Violators may be subject to fines and imprisonment.

Cal. Civ. Code § 1939.23 prohibits car rental companies from using, accessing, or obtaining information about a renter obtained using electronic surveillance technology installed in a vehicle.

Cal. Bus. & Prof. Code §§ 22948.20 -22948.25 prohibit manufacturers of "connected televisions" (defined as video devices with screen displays of at least 12 inches designed for home use and connected to the Internet) from using a voice-recognition feature in operating the connected television without prominently informing the user or the user's designee at the time of initial set-up that voice recognition is being used. Any recordings of spoken words resulting from the use of the voice recognition feature for purposes of improving the feature may not be sold or used for advertising purposes.

Cal. Lab. Code § 435 prohibits employers from recording employees in restrooms, locker rooms, or rooms designated by the employer for changing clothes.

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

Cal. Civ. Code § 1785.31 provides for a cause of action by a consumer against a person who violates the Consumer Credit Reporting Agencies Act for actual damages and, in the case of willful violations, punitive damages of $100 to $5,000 per violation.

Cal. Civ. Code § 1798.84 provides that a customer injured by a violation of the Customer Records title (see I.D.2.) may institute a civil action to recover damages and attorneys' fees, including injunctive relief, as appropriate. Such a customer also may recover a civil penalty of up to $3,000 per violation if the violation is willful, intentional, or reckless, and up to $500 per violation for all other violations.

Cal. Civ. Code § 1786.52 provides that consumers may bring a civil action in a court of competent jurisdiction against an investigative consumer reporting agency, a user of an investigative consumer report, or an informant for invasion of privacy or defamation in violation of the Investigative Consumer Reporting Agencies Act. Liability is equal to actual damages or $10,000, plus costs and attorneys' fees (Cal. Civ. Code § 1798.50).

The Consumer Protection Against Computer Spyware Act (Cal. Bus. & Prof. Code §§ 22947 -22947.6) prohibits any person from knowingly causing spyware to be installed on a computer. While the Act does not contain its own specific enforcement provisions, under the general enforcement provisions of the Business and Professions Code (§§ 17200 -17208), civil penalties and injunctive relief are available.

2. Identity Theft

Cal. Penal Code § 530.5 makes it a public offense, punishable by a fine or one year's imprisonment, for a person to willfully obtain the personal information of another and use it for any unlawful purpose.

Cal. Civ. Code § 1798.93 provides that a person may bring an action against a claimant to establish that the person is a victim of identity theft, as defined by Cal. Civ. Code § 1798.92, with respect to the claimant's claim. The statute provides that if the person proves that he or she is an identity theft victim, the person is entitled to a declaration that he or she is not liable on the claim, an injunction prohibiting the claimant from collecting on the claim, and under certain circumstances, damages and civil penalties.

Under the Fair Debt Collections Practices Act, specifically Cal. Civ. Code § 1788.18, a debt collector must cease collection activities on receipt either of a police report filed by the debtor showing that the debtor is a victim of identity theft with respect to the debt at issue, or a written statement that the debtor claims to be an identity theft victim with respect to the specific debt. The written statement must contain a variety of information specified by the statute. The debt collector must inform the consumer reporting agencies that the claim is disputed and must initiate an investigation within 10 business days after receipt of the information described above. Within 10 business days of the commencement of the investigation, the debt collector must inform the debtor whether it will proceed with, or cease, collection activities.

Cal. Civ. Code § 1748.95 and Cal. Fin. Code §§ 4002 and 22470 require Supervised Financial Institutions (e.g., banks) and finance lenders to inform an individual if another person attempts to improperly use the individual's identity.

3. Invasion of Privacy

Cal. Civ. Code § 1708.8 defines the physical invasion of privacy, which includes trespassing in order to capture a physical image, sound recording, or other physical impression of a person. It further prohibits the distribution of personal information gathered by such means. The law has been expanded to cover the use of drones for surveillance.

4. Other Causes of Action

Cal. Civ. Code § 1799.2 provides for a civil cause of action by a person against a business that violates the provisions of the Code prohibiting the disclosure of certain records by businesses performing bookkeeping services without consent. The business is potentially liable for actual damages, but in no case less than $500 plus costs and attorneys' fees. Similar provisions apply to businesses that provide video recording sales or rentals that disclose personal information (Cal. Civ. Code § 1799.3).

Cal. Civ. Code § 56.35 specifies that a patient whose medical information has been used or disclosed in violation of the Confidentiality of Medical Information Act resulting in economic loss or personal injury may recover compensatory damages, punitive damages of up to $3,000, attorneys' fees of up to $1,000, and costs.

Cal. Penal Code § 629.86 provides for a civil cause of action against anyone who intercepts electronic communications without judicial authorization. The claimant is entitled to recover actual damages of $100 per day for each day of violation or $1,000, whichever is greater, as well as punitive damages and attorneys' fees.

Cal. Civ. Code § 1798.90.54 provides that any individual injured by a violation of requirements applicable to automated license plate recognition (ALPR) operators and end-users (see I.E.11.) may bring a civil cause of action for the violation. A court may award actual damages (not less than liquidated damages of $2,500), punitive damages on proof of willful or reckless disregard, attorneys' fees and costs, and other equitable relief.

H. CRIMINAL LIABILITY

Cal. Civ. Code § 1798.57 provides that the intentional disclosure of medical, psychiatric, or psychological information in violation of the Information Practices Act is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury.

Cal. Civ. Code § 56.36(a) specifies that a violation of the Confidentiality of Medical Information Act resulting in economic loss or personal injury is punishable as a misdemeanor.

Cal. Penal Code § 530.5 makes it a public offense, punishable by a fine or one year's imprisonment, for a person to willfully obtain personal information of another and use it for any unlawful purpose.

Cal. Penal Code §§ 630 -638.55 penalize invasion of privacy through unlawful tapping, eavesdropping, recording, or opening of telephone communications or telegraphic messages. These Code provisions further prohibit nonconsensual recording or disclosure of private communications.

Cal. Penal Code § 629.84 provides for a criminal fine of up to $2,500 and imprisonment of up to one year against anyone who intercepts electronic communications without judicial authorization.

Cal. Penal Code § 502 prohibits accessing a computer, computer system, or computer network in order to control or obtain data.

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. ATTORNEY GENERAL

The California Department of Justice has a Privacy Enforcement & Protection Unit, which enforces state and federal privacy laws, provides resources to California residents and businesses, and advises the state Attorney General on privacy matters.

B. OTHER REGULATORS

Cal. Gov't Code §§ 11549 -11549.10 created the Offices of Information Security and Privacy Protection. The Office of Privacy Protection was defunded in 2012. In November 2016, Governor Brown appointed a new Chief Information Security Officer, who serves as director of the Office of Information Security.

C. SANCTIONS & FINES

Cal. Fin. Code § 4057 provides that entities subject to the Financial Information Privacy Act are subject to civil penalties of up to $2,500 per violation, with a cap of $500,000 if the disclosure involves more than one person. The penalties are to be imposed by a court of competent jurisdiction brought in the name of the people of California by the Attorney General or by the regulator with functional authority over the financial institution.

Cal. Civ. Code § 56.36(c) provides for administrative fines and civil penalties for both knowing and willful and negligent disclosures of information in violation of the Confidentiality of Medical Information Act.

D. REPRESENTATIVE ENFORCEMENT ACTIONS

In a settlement announced on March 18, 2016, Wells Fargo Bank agreed to pay $8.5 million in civil penalties, cost reimbursement, and contribution to privacy rights organizations to resolve an enforcement action in which the bank was accused of recording consumer's phone calls without informing them of the recordings. The press release announcing the settlement includes links to the complaint and stipulated judgment.

On Oct. 13, 2014, the Attorney General announced a $28.4 million settlement with Aaron's, Inc., a rent-to-own business, to resolve consumer protection and privacy violations. Among other actions, Aaron's impermissibly allowed its franchisees to install spyware without consent on laptop computers rented to its customers. The press release announcing the settlement includes links to the complaint and conformed stipulation for entry of final judgment.

A comprehensive list of recently issued privacy enforcement actions instituted by the California Department of Justice is available on the Department's website.

E. STATE RESOURCES

The California Department of Justice maintains a website that catalogs the state's privacy laws.

III. RISK ENVIRONMENT

California has a tradition of being at the forefront of privacy and security regulation and enforcement, and that is unlikely to change anytime soon. California privacy regulators and plaintiffs' attorneys have a broad and often unique array of California privacy and security laws at their disposal, from the California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §§ 22575 -22579, (mandating online privacy policies) to the "Shine the Light" Law, Cal. Civ. Code § 1798.83, (regulating disclosures for direct marketing purposes) to a particularly robust and expansive security breach notification law (Cal. Civ. Code § 1798.82). California also remains a hotbed of privacy enforcement and regulation because it is home to Silicon Valley and many of the largest tech companies.

California's activist role in privacy enforcement was demonstrated when then-Attorney General (now Senator) Kamala Harris drew attention to companies that had allegedly failed to post privacy policies for mobile applications. Under CalOPPA, Attorney General Harris issued warning letters to scores of companies believed to have inadequately addressed mobile app privacy policy issues. The California AG's position is that CalOPPA reaches all "operators of a commercial web site or online service" that gather personal information about California residents. Under the Act, an "operator" is "any person or entity that owns a Web Site located on the Internet or an online service," including mobile and social apps. Thus, for companies with websites and mobile apps, the key question is not where they are located geographically but what type of personal information – if any – is collected from its California users. The Attorney General followed the warning letters with a January 2013 guidance document, "Privacy on the Go: Recommendations for the Mobile Ecosystem."

While the mobile app privacy letters were more of a warning shot, the AG's office has also demonstrated a willingness to pursue and collaborate in large and high-profile privacy enforcement actions, most recently involving Target Corporation and Wells Fargo Bank.

In May 2017, Target Corporation, in an assurance of voluntary compliance, settled a multi-state investigation in response to allegations that over 40 million customers had their payment card information compromised during the 2013 holiday season after the company failed to provide reasonable data security. Target agreed to pay a record $18.5 million settlement; California received more than $1.4 million, the largest of any state. As part of the settlement, Target was required to adopt advanced measures to secure customers' information. The settlement required Target to employ an executive to oversee a comprehensive information security program and advise its CEO and board, encrypt or otherwise protect payment card information to make it useless if stolen, and adopt other technological measures. In addition, the settlement required Target to integrate business practices recommended in the Attorney General's Data Breach Reports previously published by the California Department of Justice.

In March 2016, Wells Fargo Bank, in a stipulated final judgment agreed to an $8.5 million settlement for violating California privacy laws by recording consumers' phone calls without a timely disclosure to consumers, as required by Sections 632 and 632.7 of the California Penal Code. This investigation and subsequent settlement agreement was a collaboration between the Attorney General's Office and five District Attorney Offices throughout the state. Wells Fargo, a California-based bank, agreed to pay $7.616 million in civil penalties and $384,000 in prosecutors' investigative costs, as well as contribute $500,000 to two organizations that advance consumer protection and privacy rights in California. In keeping with California's strong privacy-protection standards, Wells Fargo also agreed to make clear, conspicuous, and accurate disclosures when recording confidential communications between the bank and its customers, as well as implement an internal compliance program to ensure policy changes.

The California AG's office also continues to produce guidance documents staking out new issues of regulatory focus, such as "Ready for School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data," issued in November 2016. The guidance interprets and elaborates upon two California student privacy laws enacted in 2014. The first law applies to local educational agencies (such as school districts and charter schools) and requires specific terms to be included in contracts for services and software that store or collect student data, Cal. Educ. Code § 49073.1. The second law, the Student Online Personal Information Privacy Act, Cal. Bus. & Prof. Code § 22584, (known as SOPIPA), imposes obligations on companies providing education technology ("Ed Tech"). The Ed Tech industry includes (i) administrative management systems and tools, such as cloud services that store student data, (ii) instructional support, such as testing and assessment, and (iii) content, including curriculum and resources such as websites and mobile apps. Prior Attorney General guidance documents have addressed security breach response recommended practices, medical identity theft, mobile app privacy (as noted above), and protection of Social Security numbers.

Current Attorney General Xavier Becerra previously served 12 terms in Congress as a member of the U.S. House of Representatives. While in Congress, Attorney General Becerra was the first Latino to serve as a member of the powerful Committee on Ways And Means, served as Chairman of the House Democratic Caucus, and was Ranking Member of the Ways and Means Subcommittee on Social Security.

Prior to serving in Congress, Attorney General Becerra served one term in the California Legislature as the representative of the 59th Assembly District in Los Angeles County. He is a former Deputy Attorney General with the California Department of Justice. The Attorney General began his legal career in 1984 working in a legal services office representing the mentally ill.

It is unclear whether Attorney General Xavier Becerra will continue the activist privacy agenda advanced by his predecessor, former Attorney General Harris. As of this writing, no new privacy guidance documents have been issued under Becerra's administration, and the high-profile Target settlement was commenced by former Attorney General Harris in tandem with other state AG's offices.

IV. EMERGING ISSUES AND OUTLOOK

A. RECENT LEGISLATION

1. Workplace Privacy

2017 Cal. Laws 688 (enacted Oct. 12, 2017, effective Jan. 1, 2018) prohibits an employer from relying on the salary history information of an applicant for employment as a factor in determining whether to offer an applicant employment or what salary to offer an applicant, and also prohibits an employer from seeking salary history information about an applicant for employment and would require an employer, upon reasonable request, to provide the pay scale for a position to an applicant for employment.

B. PROPOSED LEGISLATION

1. Security of Connected Devices

S.B. 327, if enacted, would be the first state or federal law to generally regulate the privacy and security of Internet of Things ("IoT") smart devices. The bill would require a manufacturer that sells or offers to sell a connected device, as defined, to equip the device with reasonable security features appropriate to the nature of the device to indicate when it is collecting information and to obtain consumer consent before it collects or transmits information, as specified. The bill would require a person who sells or offers to sell a connected device to provide a notice of the device's information collection functions at the point of sale, as specified. The bill would also require a manufacturer of a connected device to provide direct notification of security patches and updates to a consumer who purchases the device. On June 1, 2017, this bill was ordered to inactive file on request of Senator Jackson.

2. Broadband Privacy

A.B 375, the California Broadband Internet Privacy Act, would prohibit broadband Internet access service providers, as defined, from using, disclosing, or permitting access to customer proprietary information, as defined. It would also prohibit those providers from refusing to provide broadband Internet access service, or in any way limiting that service, to a customer who does not waive his or her privacy rights guaranteed by law or regulation, and would prohibit those providers from charging a customer a penalty, penalizing a customer in any way, or offering a customer a discount or another benefit, as a direct or indirect consequence of a customer's decision to, or refusal to, waive his or her privacy rights guaranteed by law or regulation. On Sept. 16, 2017, the bill was ordered to inactive file at the request of Senator McGuire.

3. Invasion of Privacy

S.B. 784 would amend the Penal Code to allow a court, in a case in which a person violates Cal. Penal Code § 647(j) (which prohibits "upskirt" photography) and intentionally distributes or makes the image or recording accessible to any other person, to impose a fine in an amount not to exceed $1,000 in addition to the punishment prescribed for the violation. The bill would require the court to include economic losses suffered by the victim for costs incurred to delete, remove, and eliminate the images and recordings when imposing restitution. The governor vetoed this measure on Oct. 4, 2017.

A.B 324 would amend the same provision to eliminate the requirement that the recorded person be identifiable. Failed passage on July 11, 2017.

4. California Cybersecurity Integration Center

A.B. 1306 addresses the California Cybersecurity Integration Center (Cal-CSIC), which was created by Executive Order in 2015. The bill would establish in statute Cal-CSIC within the Office of Emergency Services to develop a statewide cybersecurity strategy for California in coordination with the Cybersecurity Task Force. The bill would also provide that Cal-CSIC would have the same primary mission as Cal-CSIC as created by Executive Order. The measure was vetoed by the governor on Oct. 11, 2017.

5. Electronic Communications

A.B. 165 would amend California's Electronic Communications Privacy Act to specify that a government entity may access electronic device information by means of physical interaction or electronic communication with the device where the owner or authorized possessor of the device is a pupil enrolled in kindergarten or any of grades 1 to 12, inclusive, and the government entity seeking access to the device is a local educational agency, as defined, or an individual authorized to act for or on behalf of a local educational agency seeking a pupil's electronic device information or a pupil's electronic communication information when investigating alleged or suspected pupil misconduct pursuant to specified provisions.

A.B. 608 would amend California's Electronic Communications Privacy Act to specify the manner in which unrelated information obtained pursuant to a warrant is to be sealed, and by whom. The bill would also clarify that the information may be retained, before being destroyed or returned, destroyed, through the conclusion of any proceeding, including appellate proceedings.

C. OTHER ISSUES

1. Data Breach Report

In February 2016, then-Attorney General (now Senator) Kamala Harris issued the most recent California Data Breach Report, in which a variety of safeguards constituting a "reasonable level" of information security were listed. While the report does not have the force of law or regulation, it does indicate the expectations of the state's Department of Justice and specifies that the 20 Critical Security Controls defined by the Center for Internet Security represent the minimum security level that California businesses should meet. These statements regarding reasonable security expectations may inform the DOJ's future enforcement of California's "Reasonable Security" law (Cal. Civ. Code § 1798.81.5(b)). Although the "Reasonable Security" law was one of the first general state data security laws, it has thus far not been actively enforced. The statements in the 2016 California Data

Breach Report might indicate that the “Reasonable Security” law will be more vigorously enforced in the future.

2. Ballot Initiative

A ballot initiative proposed in September 2017, known as the California Consumer Privacy Act of 2018, would allow California consumers to know what personal information businesses are collecting from them, what they do with it, and to whom they are selling it. The backers of the initiative are aiming for a spot on the November 2018 statewide ballot. The measure would establish a consumer’s right to request that a business disclose what categories of personal data it gathers, and to say no to the sale of any of that information without fear of losing services or facing discrimination. It would require businesses to make those disclosures free of charge within 30 days. If enacted, the measure would represent a sea change in privacy regulation for companies doing business in California.

