Protecting Privacy while Allowing Innovation, Information Sharing Remains Challenge in Evolving Area

As Californians increase their daily interaction with technology, the public policy conversation around personal information and information security continues to take on a more prominent role. Personal information has been the subject of many laws and regulations over the last decade and new technology is constantly changing the landscape of how information is used, shared, protected, transmitted and disposed. Safeguarding electronic information is challenging; what is considered safe and adequate protection this month often is outdated the next.

California Leads Way on Information Security

Trying to stay up-to-date in this new world of rapidly changing technology is a full-time effort, but California has been at the forefront of protecting information.

In 2003, California was the first state in the nation to mandate data breach notifications. Today, there are numerous California privacy laws covering a wide variety of circumstances, ranging from how a business shares customer information to privacy provisions governing "black box" data event recorders in cars newer than 2004. In short, California is far ahead of federal law when it comes to privacy, and other states are beginning to pass laws based on California provisions, although with variations. Those variations cause national companies to grapple with numerous and varying privacy laws, which is time consuming and expensive.

Over the last few years, both the state and federal governments have examined and proposed legislation on a number of different privacy and technology issues, including large data breaches, data security requirements, cybersecurity, consent and disclosure policies for personal information, and drones. Although legislation addressing these issues passed in 2015 and 2016, this policy area will continue to develop into the foreseeable future.

Data Breaches

Recent and highly publicized data breaches involving both government and business have fostered an air of uncertainty regarding the collection, storage and use of personally identifiable information. Breaches with the most media attention—outside of the presidential election—involved large U.S. retailers and compromised customer credit card information. It is important to note that, generally, these breaches did not involve identity theft, which is different from credit card theft, although the two often are confused with one another. *Identity theft* is the unauthorized use of another person's personal identifying information to obtain credit, goods, services, money or property. *Credit card theft*, however, results when a credit card or credit card number is used by an unauthorized person to buy goods or services, usually for a short period before the victim, retailers or banks discover the misuse and close the account. The latter generally results in no financial loss to the consumer as compromised cards are replaced and accounts refunded.

As large data breaches continued to occupy headlines, both the federal and state government held hearings and introduced legislation.

Federal Activity

At the federal level, the focus remained on creating a national data breach notification standard. The U.S. Senate Banking and Judiciary committees and the U.S. House of Representatives Energy and Commerce Committee all held hearings on data breach issues in 2014 and recommended, amongst other proposals, developing a national standard for consumer notification.

Both the U.S. Senate and the U.S. House introduced different versions of the Data Security and Breach Notification Act of 2015. One of the policies driving these legislative efforts is to eliminate the patchwork of state laws that currently govern notifications. When data breaches do occur, businesses must comply with the state law where the consumer resides. Data breaches, particularly for large companies, often involve consumers in multiple states. With 47 different breach notification laws across the nation, compliance with each jurisdiction creates significant burdens, costs and litigation risks for businesses. Enacting a national standard would alleviate a number of these issues and provide notice consistency to consumers. Ultimately, the proposed federal legislation did not move forward.

With the current partisan gridlock and disagreement amongst stakeholders, enacting a uniform federal data breach law remains a significant challenge. One of the primary issues with a national standard is the debate over the federal preemption needed to create the desired uniformity. States with more stringent laws have fought against past efforts, arguing that the proposed federal legislation weakens consumer protections. A balance between uniformity and consumer protections must be struck amongst the current state laws in order to move forward with federal legislation.

CalChamber

Expanding Opportunity
An Agenda for All Californians

2017 Business Issues and Legislative Guide

See the entire CalChamber 2017 Business Issues and Legislative Guide at
www.calchamber.com/businessissues
Free PDF or epub available to download.

Special Thanks to the Sponsors
Of the 2017 Business Issues and Legislative Guide

Premier

Chevron

Bronze

enterprise

Iron

AUTOMOBILE CLUB • SOUTHERN CALIFORNIA • AAA
We're always with you.®

COMCAST BUSINESS
B4B
BUILT FOR BUSINESS™

California Legislation

In California, recent data breach legislation has involved creating more prescriptive notification requirements and new notice triggers. A bill introduced in 2015 sought to mandate a specific form for breach notifications, and would have required businesses to utilize a one-page format containing the statutorily required information. The policy behind the bill had merit; the author's intent was to make breach notifications easier to read and understandable for consumers. The bill, however, created significant compliance issues. As described above, businesses must comply with up to 47 state notification laws for a single breach. To ensure compliance, businesses often draft notices that satisfy all or nearly all jurisdictions. The legislation essentially would have created a prescriptive California-only form that would not have satisfied many other state notification laws, thereby increasing notification burdens and costs.

The California Chamber of Commerce initially led a coalition in opposition to the bill, but was able to reach a compromise with the author that makes notifications more consumer-friendly while maintaining the flexibility in the structure for businesses issuing notices in multiple states. The amended version of the bill was signed into law by Governor Edmund G. Brown Jr., but represents another example of the need for a national data breach law.

In 2016, AB 2828 (Chau; D-Monterey Park; Chapter 337) created new breach notification triggers for encrypted personal information. Under then-current law, encrypting information creates a safe harbor from data notification laws—notification is not required if the breached information was encrypted as there is no risk of harm to the consumer. AB 2828 clarified, however, that if both encrypted personal information and the encryption key has been acquired by an unauthorized person, and the key could render the information readable or usable, then businesses must provide breach notifications. The CalChamber did not oppose this bill, recognizing that the loss of the encryption key coupled with the breach of personal information could potentially harm consumers and, as such, should trigger notification.

Data Security

Data security legislation also took a prominent role over the last legislative session. While data breach laws prescribe what businesses and government agencies must do when breaches occur, data security laws focus on the level of protection organizations must provide to personally identifiable information (PII). Current law requires businesses to "provide reasonable security" for PII, which is defined as an individual's first initial or first name and last name in combination with one or more of the following: 1) Social Security number; 2) driver license number or identification number; 3) credit card information; or 4) medical information.

A bill introduced in 2015, AB 83 (Gatto; D-Glendale), sought to further define "reasonable security" and expand the data components contained within the PII definition. Currently, no statutory definition exists for "reasonable security" and there is a dearth of case law explaining what level of protection is needed for compliance. AB 83 created a factor test to evaluate security measures. This factor test was similar to the national data security standard proposed by President Barack Obama's administration. It would have required businesses to secure PII "to the degree that any reasonably prudent business would." At a minimum it requires businesses to:

- Identify the foreseeable risk to the information;
- Establish, implement, and maintain safeguards;
- Regularly assess the sufficiency of the safeguards; and
- Evaluate reasonableness of the security procedures in light of the type of information, the foreseeability of threats, the existence of widely accepted practices and the cost of implementing, and regularly reviewing the safeguards.

Conceptually, the CalChamber and the business community did not have an issue with these requirements. The business community remains focused on flexibility in data security laws. Codifying any specific security technology or procedure will stymie advancements needed to keep up with ever-evolving and sophisticated security threats.

The CalChamber initially opposed the second part of the bill that expanded the definition of PII. Each expansion requires significant costs and resources, and brings litigation risk associated with protecting the new information and providing notices if it is breached. As such, expansion of the PII definition should be limited to information that would be harmful to consumers if misused and each additional PII element should be defined precisely.

Some of the new data elements in AB 83 did not meet these requirements and either were benign to the consumer or imprecisely defined. The CalChamber led an industry coalition that worked with the author's office throughout the legislative session to find a viable solution to the expansion of the PII definition. The CalChamber removed its opposition to the bill after new definitions for "biometric information" and "geolocation information" were amended into the bill.

Ultimately, AB 83 stalled in the Senate Judiciary Committee. It is expected, however, that similar legislation will be introduced in 2017.

In addition to legislation, the California Attorney General provided recommendations on reasonable data security standards for businesses as part of the yearly *California Data Breach Repor*t. The report states that "[t]he twenty controls listed in the Center for Internet Security's Critical Security Controls define a minimum level of security" for businesses, including small businesses. The report also recommends that businesses: 1) utilize multi-factor authentication for critical systems, data and consumer-facing online accounts; 2) encrypt data in transit; and 3) encourage individuals affected by breach of Social Security and driver license numbers to place fraud protections on their credit files.

Although these recommendations do not create legal

requirements, courts may rely on them in interpreting "reasonable security" under the California Civil Code, which, as previously mentioned, lacks a definition in statute or existing case law. These recommendations also may wind up in future data security bills.

Cybersecurity

Late in 2015, President Obama signed into the law the Cybersecurity Information Sharing Act (CISA) as another tool to combat malicious breaches and hacks. CISA encourages businesses, government agencies and other entities to share cybersecurity threat information with each other. Swift distribution of this information will allow organizations to better react and defend against further and future attacks.

The major hurdle to information sharing has been litigation exposure faced by organizations when handing over personal data as part of sharing information about the threat. To address this issue, CISA limits the liability when sharing information in compliance with CISA. It also balances this safe harbor with increased privacy protections. Previous versions of CISA failed to make it through the Senate after President Obama threatened a veto due to what he viewed as a lack of privacy protections.

New California cybersecurity legislation in 2016 included criminalizing "ransomware" (SB 1137; Hertzberg; D-Van Nuys); implementing a "bug bounty" modeled after private industry for the state computer systems (AB 2720; Chau; D-Monterey Park); and requiring the California Office of Emergency Services to develop a statewide response plan for cybersecurity attacks on critical infrastructure (AB 1841; Irwin, D-Thousand Oaks).

SB 1137 and AB 1841 were signed into law (Chapter 725 and Chapter 508), while AB 2720 failed to move out of the Assembly Appropriations Committee.

Notice and Consent

The debate continues over what constitutes sufficient notice for collecting, storing or using information and how to effectively provide this information to the consumers. Current law requires businesses that collect personal information to develop and conspicuously post privacy policies. As a matter of practice, most businesses also seek consumer consent before collecting information. This is another area in privacy policy, however, where consumer protection and demand for innovation must be balanced carefully.

AB 2623 (Gordon; D-Menlo Park) highlighted the difficulty in this balance. On its face, the bill attempted to provide more clear and concise disclosures to the consumer by modeling new privacy policy requirements after a federal law that requires a brief table of certain financial data for credit card agreements and marketing—commonly known as a "Schumer box." The Schumer box condenses important financial information into a short, easy-to-read format. The Schumer box works well for presenting information that is easily and precisely defined by numbers.

The issue with AB 2623 was that privacy policy information is inherently different than financial data. Privacy policies contain qualitative descriptions about the different types of personally identifiable information and how that information is collected, utilized and/or shared—this information cannot be accurately distilled to numbers or a few words. By attempting to rigidly limit these descriptions, the bill would have resulted in incomplete privacy policies, thereby preventing consumers from receiving critical information or leaving them with a misunderstanding of the privacy policy.

The CalChamber led a coalition in opposition to AB 2623, and it eventually was amended with language unrelated to privacy policies.

Stakeholders and policymakers continue to grapple with the issue raised by AB 2623: how to provide comprehensive and understandable notice to consumers. Due to constantly evolving technology, more legislative mandates that create one-size-fits-all policy requirements are not the answer. Businesses continue to develop innovative approaches and best practices for providing consumers with meaningful privacy disclosures, including providing multiple just-in-time disclosures made at relevant times to consumers. These disclosures vary by industry based on consumer needs and interactions with different products and services, requiring privacy disclosure rules and regulations to remain flexible.

Drones

The proliferation of unmanned aerial vehicles (commonly known as drones) for commercial use and by hobbyists has prompted state legislatures and the federal government to address this burgeoning policy area. Industry reports forecast that the commercial drone market will grow to $127 billion worldwide, with drone usage touching nearly every sector and industry. Some notable commercial uses include:

- **Delivery/Shipping**: A number of companies are developing technology to deliver packages quickly.
- **Infrastructure Inspection/Monitoring**: Drones can be utilized to monitor pipelines, power lines, facilities, wind turbines and ports. Drones will potentially reduce health and safety risks for these dangerous activities.
- **Disaster Response**: The small size and mobility of drones allow them to travel into dangerous areas during natural disasters or other emergencies. Drones can assist first responders by locating individuals, surveying damage and ongoing threats, and delivering supplies.
- **Agriculture Monitoring**: When there are vast amounts of land, crops and livestock to monitor, drones are an efficient tool to survey acreage and collect information. For example, drones are useful in water management, allowing farmers to track irrigation issues and soil hydration—a critical function in California's drought. Drones also can help with detecting crop disease and targeted spraying of pesticides.
- **Insurance Claims**: Drones allow insurance companies to quickly and safely evaluate and document property damage after

an accident or natural disaster. This will reduce recovery time for the insured.

• **Real Estate/Construction**: Drones enable easier access to aerial photography for marketing property and developing construction projects.

• **Film and Television Production**: Drones already are being used by the entertainment industry to film scenes that previously would have been too dangerous or cost prohibitive.

• **Security**: Drones permit the monitoring of large facilities—such as a college campus or mall parking lot. Abnormal activity or threats can be recorded instantly and law enforcement notified.

With the anticipated expansion in drone usage, there also have been a number of safety and privacy concerns. These concerns include dangerous interference with commercial flights, hazards to individuals and property on the ground from a malfunctioning drone, and recording or monitoring of individuals and personal property.

Federal Regulation

Earlier in 2016, the Federal Aviation Administration (FAA) finalized regulations on commercial drone usage. These regulations include airspace restrictions, operator certification, line-of-sight requirements, and freight and speed limits. To the extent these regulations interfere with business operations, businesses can apply rules that the FAA will evaluate on a case-by-case basis, granting waivers where businesses demonstrate the proposed use will be safe. To date, more than 75 of these waivers have been granted.

The FAA will continue to develop drone rules and anticipates soon releasing rules governing commercial drone flight over people.

California Legislation

According to the Association for Unmanned Vehicle Systems International (AUVSI), 266 state bills related to drones were introduced throughout the country as of July 2016. The California Legislature introduced 23 of these bills during the last legislative session. The range of topics covered by these bills included flight area restrictions, insurance requirements, prohibitions on interference with first responders, technological capabilities, privacy rules, state preemption, accident reporting, and use by law enforcement.

Ultimately, only six of these bills made it to Governor Edmund G. Brown Jr. He signed two and vetoed four. The CalChamber did not take a position on either bill signed into law. In his veto messages, Governor Brown made clear that he prefers a comprehensive approach to drone regulation that takes into account FAA rules, not a piecemeal approach that creates conflicts amongst local, state and federal regulations and statutes.

The CalChamber supports Governor Brown's call for uniformity. Rules protecting safety and privacy may be needed in the coming years as drones become more ubiquitous and the industry continues to grow. Policymakers should not encumber innovation by rushing to pass premature, unnecessary or conflicting legislation.

What to Expect in 2017

Employers can expect another busy year for privacy and technology legislation in 2017. During the last legislative session, the California State Assembly created a new standing committee on Privacy and Consumer Protection due to the increasing number of privacy and technology bills, and the need for a specific focus on these issues.

Bills likely will be introduced to: regulate online brokers and the big data industry; expand the definition of personal information; codify data security standards; clarify data breach rules and responsibilities; prescribe additional disclosures in privacy policies; mandate specific types of consent in order to collect or use certain data; modify information sharing among affiliated businesses and partners; and develop rules on drone usage.

Additionally, more pressure to push legislation likely will come from national privacy groups that view California as the most likely jurisdiction to pass new legislation. With the partisan gridlock at the federal level and the change in presidential administrations, enacting new national privacy laws will continue to prove challenging. The California Legislature, however, has historically been more receptive to enacting these types of proposals. Also, as a large state that is home to the technology industry, California often serves as a model for other states' privacy legislation.

CalChamber Position

The CalChamber supports protection of privacy rights and privileges, uniform national laws, and regulations governing privacy issues. Increased penalties and incarceration for thefts of personal information are proper for violations.

The CalChamber supports the development of industry standards for protecting data rather than embedding static technology in statute; the ability for companies to securely share information; effective privacy policy and data usage rules that do not stifle innovation; and the continued advancement of drone technology.

Article written by Jeremy Merz while serving as CalChamber policy advocate. He now is vice president, state affairs – western region at the American Insurance Association.

Staff Contact
Jeanne Cain
Executive Vice President, Policy

jeanne.cain@calchamber.com
California Chamber of Commerce
P.O. Box 1736
Sacramento, CA 95812-1736
(916) 444-6670
www.calchamber.com
January 2017