7 Calif. Privacy Bills To Watch

By **Erin Coe**

Law360, San Diego (June 5, 2015, 3:08 PM ET) -- California lawmakers are set to consider a host of measures this year that could fuel privacy litigation, including a proposal requiring businesses to boost privacy protections for stored personal information like geolocation data. Here, attorneys point to seven bills that could alter the privacy landscape in the Golden State.

Geolocation Legislation

A.B. 83, carried by state Assemblyman Mike Gatto, D-Los Angeles, seeks to expand the list of personal information that businesses have to protect to include geophysical location data, such as Uber travel logs. The measure also **lays out** "reasonable security procedures and practices" that businesses would need to follow to safeguard personal information, which also includes Social Security numbers, driver's license numbers, and financial and medical information. It cleared the state Assembly floor in May on a 66-4 vote.

"The bill is specific about the standards that California is going to measure businesses against for privacy and security," said Sharon Klein, a partner at Pepper Hamilton LLP. "If the bill passed, it would really inform the business community, and because of that, it would encourage greater adoption to security compliance efforts."

A.B. 83 would require businesses to identify reasonably foreseeable internal and external risks to privacy and security of personal information, establish safeguards that would protect against unauthorized use, and regularly assess the sufficiency of safeguards.

Businesses have already raised questions at the federal level about what standards they must meet in safeguarding customer information. Wyndham Worldwide Corp., which **is fighting** a Federal Trade Commission suit over its security measures, has criticized the government for pursuing an enforcement action even though it hasn't published standards of care to help companies avoid violations, according to Klein.

“California is trying to get a jump on that argument by saying what the standards are, and I think that is progress for companies that are trying to understand what their compliance obligations are,” she said.

At the same time, the measure has the potential to drive up privacy litigation against businesses, she said.

“It essentially sets data points for the government to enforce,” she said. “It helps businesses understand where they need to concentrate their efforts, and it also helps the government eliminate defenses in litigation.”

Another bill, **S.B. 576**, would build on the California Online Privacy Protection Act by requiring mobile application operators to provide clear and conspicuous notice to consumers on the collection of geolocation information. Operators also would have to obtain users’ affirmative express consent before collecting and sharing that data. The measure was introduced by state Sen. Mark Leno, D-San Francisco, in February, but has been held over as a two-year bill and will be heard in January.

“Geolocation information is such a critical commodity in the mobile app ecosystem,” W. Reece Hirsch, a partner at Morgan Lewis & Bockius LLP, said. “It’s valuable and can color which ads are served to consumers. Right now, there is no uniform requirement for mobile app operators to provide robust notification that geolocation data is being collected.”

Cal OPPA requires that website operators post an online privacy policy, and while the California attorney general has said the law applies to mobile apps as well, this bill would cement that interpretation, Hirsch said.

Data Breach Response Legislation

A.B. 259, carried by state Assemblyman Matt Dababneh, D-Encino, would require a government agency that suffers a data breach to offer at least a year of identity theft prevention and mitigation services free of charge to affected consumers. The bill cruised out of the state Assembly on June 1 on an 80-0 vote.

A few years ago, companies generally would offer identify theft prevention and mitigation services to an individual only if fraud or identity theft had been committed, but it has become

increasingly common for companies, regardless of size, to offer some services in the event of a breach, according to Hirsch.

“California was the first state to pass a data security and breach notification law, and we continue to keep the law on the cutting edge by going back and revising it to reflect emerging best practices,” he said. “Other states may be interested in picking up on the idea and adopting it in their own legislation.”

Between 2012 and 2014, 10 California agencies reported breaches, including the state Department of Justice, the Employment Development Department, the Department of Motor Vehicles and California State University.

The bill also sheds light on an existing law that directs businesses that issue breach notifications to offer “appropriate identity theft and mitigation services, if any,” to affected individuals at no cost, according to Catherine Valerio Barrad, a partner at Sidley Austin LLP. The bill seeks to use the same wording as that law.

Some have interpreted “if any” to mean that if no identity theft prevention services are appropriate, a business is not required to offer them, such as when the breach involves disclosure of a credit card number and affected consumers have obtained new credit cards with different numbers. Others believe the law means that businesses may offer such services but are not required to.

“In the committee analysis of A.B. 259, there’s discussion that the purpose of the wording is to require the offer of such services if they would be appropriate,” she said. “This interpretation affects how I advise my corporate clients on how to read the existing law. My advice to them is that the only time they are not required to offer services is if there aren’t any that are appropriate.”

Eavesdropping TV Legislation

A.B. 1116, introduced by Gatto, would **require** that smart-TV makers ensure voice-recognition features can’t be enabled without the consumer’s consent and would bar them from using recorded conversations for advertisement purposes. The state Assembly approved the bill in May on a 74-0 vote.

The bill deals with voice recognition on connected TVs, which have been on sale in the United States for only a few years. Gatto **told Law360** in May that while most consumers know that searching for products online could lead them to receive targeted ads, they may not realize that appliances in their homes may incorporate technology based on a similar model.

The measure empowers the state attorney general or a district attorney to prosecute manufacturers that fail to implement proper privacy safeguards. The officials could seek injunctive relief as well as a civil penalty of up to $2,500 per violation. The bill notes that it doesn't create a private right of action.

The measure, if passed, could lead to litigation if smart TVs fail to perform as advertised, such as if voice-recognition features are activated without the consumer's consent or if voice data is used for marketing and advertising purposes, according to Barrad.

"If consumers choose a setting to keep their TV from recording something, but they later suspect that the TV has recorded them or that their recordings have been used to serve advertising on them, a company might face a lawsuit based on existing statutory or common law privacy protections," she said.

Digital Privacy Legislation

Drawing support from Google Inc., Facebook Inc. and other tech companies and advocacy groups, **S.B. 178** would require law enforcement to **obtain a search warrant**or wiretap order before accessing private communications and location data stored on smartphones, tablets and other digital devices. The measure, known as the California Electronic Communications Privacy Act, passed out of the state Senate on Wednesday on a 39-0 vote.

Under the bill, law enforcement would be barred from accessing a person's digital information, which the proposed bill broadly defines to encompass personal messages, passwords, personal identification numbers, GPS data, photos, medical and financial information, contacts, and metadata, without a warrant based on probable cause. It was proposed by Leno and state Sen. Joel Anderson, R-San Diego.

Leno proposed a similar measure, S.B. 467, in 2013, but Gov. Jerry Brown vetoed it, saying

its notice requirements went beyond federal law and could impede ongoing criminal investigations.

“The bill has broad support from companies and organizations who have been asking for parity in the privacy laws governing online and offline communications,” said James Snell, a partner at Perkins Coie LLP. “It would add protections to electronic communications for users, and clarify the rules for production for providers and law enforcement.”

If passed, the measure could lower the risk of liability for providers of communication services and devices, according to Snell.

“Cal ECPA could reduce privacy litigation because it would provide a safe harbor for companies who produce information in accordance with the terms of a search warrant,” he said.

Drone Legislation

In light of the federal government’s plan to integrate unmanned aerial vehicles into the national airspace this year, a flurry of California measures have been introduced, including one bill that would ban trespassing on private property with unmanned aircraft systems.

S.B. 142, carried by state Sen. Hannah-Beth Jackson, D-Santa Barbara, would **broaden the definition of trespassing** to include using the vehicles below navigable airspace of 400 feet on private property without permission and subject violators to civil damages. It gained approval from the state Senate in May on a 24-9 vote.

“Drones can have a lot of very intrusive applications,” said Mark Mao, co-chair of Kaufman Dolowich & Voluck LLP’s technology practice. “The measure tries to protect people from being snooped on by drones.”

Another measure, **A.B. 14**, would create a task force to establish policy for unmanned aircraft systems. The bill was introduced by Assemblywoman Marie Waldron, R-Escondido, in December, but the Assembly Transportation Committee chair voiced concerns that it was unclear what a separate task force would provide that couldn’t already be accomplished by the legislative process. As a result, the bill has been held over as a two-year bill and will be heard in January.

The formation of a task force could encourage a more consistent approach to drone bills, according to Barrad.

“A task force could recommend comprehensive policy that might drive the structure of legislation addressing UAVs in the future,” she said.

--Editing by Kat Laskowski and Emily Kokoll.