

California Considers Data Security, Geolocation Rules

By Laura Mahoney

Aug. 22 — Companies such as Uber Technologies Inc., Lyft Inc. and Fitbit Inc. would have to protect consumer biometric and geolocation data under a bill recently revived and amended in the California state Senate.

The bill would require companies doing business in California to meet a “reasonably prudent” standard for data security safeguards and expand the definition of protected personal consumer data to include geolocation and biometric information.

Assemblyman Mike Gatto (D) amended A.B. 83, a bill that has been dormant for a year, setting new standards for businesses to use reasonable security procedures and practices if they hold or maintain personal information.

The bill passed the Assembly in 2015, and now needs approval in the Senate and agreement from the Assembly on the amendments to reach the desk of Gov. Jerry Brown (D).

Although the bill hasn't moved since July 2015, Gatto told Bloomberg BNA Aug. 22, the new amendments reflect a compromise he negotiated for two years with business and privacy groups that still accomplishes his intent to set California state standards for protecting personal data where none now exist.

“The next frontier is to use facial recognition to track you when you walk into a mall,” he said. “People who store this information should have strong encryption and consumer protections.”

Foreseeable Risks

Under the bill, businesses that hold personal consumer information would be required to identify foreseeable internal and external risks that could compromise the information, and maintain reasonable safeguards.

The bill would expand the definition of personal information in California law beyond social security numbers, driver's license numbers and medical information to include geolocation and biometric data, tax identification numbers, passport numbers, military identification numbers, and employment identification numbers.

Gatto said crafting the geolocation data provisions to cover consumer data without going too far has been tricky. For example, the bill would apply to data gathered by Uber, Lyft and Fitbit's exercise trackers. It wouldn't apply to data from key card readers for entering office buildings, or electronic receipts that indicate a person's location.

"We're not trying to subsume key card readers at different entrances on different floors at law firms," he said.

Reasonably Prudent

The bill would require businesses to use reasonable security procedures and practices for the storage and transmission of data, which means, under the bill, "security of that information to the degree that any reasonably prudent business would provide."

Businesses would have to regularly assess the sufficiency of their safeguards, which would be based on the type of information under their control, foreseeable threats, the existence of widely accepted practices, costs and the size of the businesses.

Health-care providers and plans, financial institutions and entities covered by the Health Insurance Portability and Availability Act would be exempt under the bill.

The measure doesn't contain specific penalties, but Gatto said enforcement would happen in one of three ways: through the California Attorney General, through civil suits under Business and Professions Code Section 17200—which applies to unfair competition—and civil suits for negligence.

Gatto said he is expecting that the Senate Judiciary Committee, which approved the earlier version of the bill in July 2015, will consider the bill again this week because of the substantial amendments. If it passes the committee, it will need approval on the Senate floor and a final vote from the Assembly to concur in the Senate amendments before it can reach the governor's desk.

The session ends Aug. 31.

Full text of A.B. 83, as amended for Senate review, is available at http://www.leginfo.ca.gov/pub/15-16/bill/asm/ab_0051-0100/ab_83_bill_20160819_amended_sen_v94.pdf