Pending amendment to California data privacy law would extend protection to geophysical location and biometric data

By Karl D. Belgum and Sterling Chan

A bill is advancing through the California legislature that would expand privacy protection to two new categories of personal data: geophysical location information and biometric data. The bill reflects an increasing interest in geophysical location information as a protected form of personal data and, whether it passes or not, it is unlikely to be the last word on the subject. It also attempts to provide further guidance on what specific actions a company needs to take to “reasonably secure” personal information.

Background

AB 83, introduced in the California Assembly in January 2015, would amend the basic California commercial data privacy law, Cal. Civil Code 1798.81.5. As currently written, that law imposes a duty on any company that “owns” or “maintains” “personal information” pertaining to a California resident to “maintain reasonable security procedures and practices” with respect to such data, and to extract a contractual commitment from business partners with which it shares such data to do the same. “Personal data” is defined to mean an individual’s name when combined with any of the following components: social security number, driver’s license, credit card or similar account information, or “medical information” (further defined). The existing law does not define “reasonable security procedures” except to state that they must be “appropriate to the nature of the information” and that the data must be protected against unauthorized “access, destruction, use, modification, and disclosure.” Id. The law provides a damage remedy to anyone who is injured by breach of these obligations, but there is no civil penalty or liquidated damages provision. C.C.P. 1798.84(b).

AB 83 expands protection to geographical location information

AB 83 amends the law by adding two new categories of data, which, when combined with an individual’s name, would constitute protected “personal information.” The first is “geophysical location information,” defined as “any location data generated to assess the past or current location of, or travel by, an individual, including but not limited to, geographic coordinates, street address, or WiFi positioning system.” This expands on the definition in an earlier version of the bill, which was
limited to information regarding the “duration of a transport service” or “location and route of a transport service.” So, while the bill previously was targeted at the transportation industry, it now applies more broadly.

If AB 83 becomes law it will be one of the first on the subject. Prior legislative efforts to limit commercial and governmental procurement and disclosure of geolocation data have not met with much success. On the federal level, the proposed Geolocation Privacy and Surveillance Act (GPS Act) would require government agencies to obtain a warrant for GPS user geolocation data, and prohibit businesses from disclosing such data about its customers without consent. The GPS Act failed passage in Congress twice, but was reintroduced again for consideration in January 2015. On the state level, both Maine and Montana state laws require law enforcement to get a warrant for obtaining geolocation data from an electronic device.

Interest in geophysical location data as a privacy issue is growing. The Federal Trade Commission (FTC) brought an enforcement action against mobile app developer Goldenshores Technologies, for deceiving users of its mobile flashlight app by sharing their geolocation data with third parties without user knowledge or consent. Goldenshores ultimately settled with the FTC, but a key part of the settlement agreement is the requirement that the company disclose its practices, and obtain separate consent from users before collecting and sharing geolocation data. Underscoring the seriousness with which the FTC takes the issue, in March 2015, FTC Bureau of Consumer Protection Director Jessica Rich testified before a subcommittee hearing of the House Energy and Commerce Committee that the definition of “personal information” should include precise geolocation data.

Cases are beginning to emerge in the courts as well. In May 2015, a former employee of California wire-transfer company, Intermex, filed a lawsuit alleging that she was fired for uninstalling a mobile app that allowed the company to track her location on Google Maps. The lawsuit alleges that Intermex asked their employees to download the Xora app to their smartphones, and the app’s GPS function allowed Intermex supervisors to see where an employee has been, their routes, as well as their real time location 24/7, even while the employees are off-duty. The claims against Intermex include invasion of privacy and wrongful termination, and the former employee is seeking damages of $500,000. The Intermex lawsuit is a cautionary illustration to businesses that utilize tracking technology to monitor their employees.

AB 83 will obviously affect entities that provide transportation services (i.e., airlines, rental cars, taxis), and newer ridesharing services such as Uber and Lyft. It may also affect auto manufacturers.

---

1 GPS.Gov-Official U.S. Government information about the Global Positioning System (GPS) and related topics, GPS Act, available here.
4 Anne Flaherty, FTC says flashlight app left consumers in the dark, NBC NEWS (Dec. 5, 2013), available here.
6 David Kravets, Worker fired for disabling GPS app that tracked her 24 hours a day [Updated], ArsTechnica (May 11, 2015), available here.
7 Adriana Gardella, Employer Sued For GPS-Tracking Salesperson 24/7, Forbes (June 5, 2015), available here.
8 Id.
who put geolocation devices in their vehicles. However, especially as recently amended, it will also apply to companies such as Google and Apple, which provide mapping and routing services to millions of users across a variety of different platforms. Indeed, a huge component of Internet business consists of delivering advertising to mobile device users based in part on their location. The obvious course for such enterprises to follow would be to make sure the name of the individual is never transmitted in tandem with geophysical location data, because the data is only protected under the California law if those two components are linked together.

**Biometric information**

AB 83 would also expand the definition of “personal information” to include “biometric” data. If AB 83 becomes law, California would join Wyoming and Illinois in pioneering legislation specifically designed to regulate the collection and safeguarding of biometric data. In California’s case, the biometric data referred to in AB 83 means not just fingerprints but any “automatic measurement of an individual’s biological characteristics.” The inclusion of the phrase “automatic” reflects some attempt to limit the scope of the provision, but still questions remain. Would photographs be biometric data? What about measurements, height and weight, or references to gender? As an illustration of the types of litigation these questions may spawn, class action suits have already been filed against Facebook and Shutterfly in Illinois claiming that the companies’ facial recognition software violates the Illinois law.

**Guidance on “reasonable security procedures”**

Finally, the bill attempts to define what constitutes “reasonable security procedures and practices.” This section reflects the constant tug of war in the legislature between those who want to mandate specific security procedures and technologies, and those who want to limit legislative pronouncements to more general “reasonableness” tests. An earlier version of the bill specifically required encryption of data, but that provision was dropped along the way. The bill now requires essentially a “process forcing” approach. Instead of requiring specific technological steps, it requires businesses to identify reasonably foreseeable internal and external risks, establish safeguards to protect against those risks, and then periodically “assess the sufficiency” of those safeguards. An enterprise must also evaluate any “material changes in operations” that may affect its risk profile. Then, when all that is done, the resulting data security procedures are measured against a combined reasonableness and best practices standard. The procedures must be reasonable in light of the type of information involved and the foreseeability of threats, and must reflect “widely accepted practices” for protecting personal information.

The guidance may not be very concrete, but the new statutory language will provide handy talking points for plaintiff’s counsel, who will plead that failure to follow one or more of the above steps led to a specific data breach. The statute certainly puts a premium on every company having a report in its files documenting that it has gone through a risk assessment process on a periodic basis and actually followed up on the results of that analysis. Failure to have such a study in the file, or failure to follow up on the risks identified by such a study, will be cited as evidence of negligence.

---


Reception to the bill

When A.B.83 was referred to the California Assembly Committee on Consumer Protection and Privacy, both the Utility Reform Network (TURN) and the Privacy Rights Clearinghouse (PRC) submitted letters to support the bill. TURN supports A.B.83’s mandate for businesses to continually meet the highest standards for data protection due to its concern for major data breaches in recent years exposing the vulnerability of personal information maintained by large entities. Similarly, PRC expressed that A.B.83 would help assure Californians that their personal information is responsibly handled by businesses. Both organizations support the idea that geolocation and travel data should be included in the definition of private data. The Committee’s analysis report does not note any opposition to the bill on file, and ultimately the bill passed through the state assembly in May 2015. Currently, A.B.83 is in the California state senate, and has been referred to the Senate Judiciary Committee. The bill must be passed by September 11, 2015, before it dies for lack of action. Should the bill’s momentum continue, it will be the law in California beginning in 2016.

For more information on the content of this alert, please contact your regular Nixon Peabody attorney or:

— Karl Belgum at kbelgum@nixonpeabody.com or (415) 984-8409
— Kate A.F. Martinez at kmartinez@nixonpeabody.com or (585) 263-1332