California Adopts "Do Not Track" and Expanded Data Breach Notification Laws

2013-09-30

On Friday California Governor Jerry Brown signed into law the second and third of a cluster of four privacy and data security bills recently passed by the state legislature, continuing California's role as among the most active states in extending the reach of on-line privacy and information security regulation. The laws signed on Friday (i) require commercial websites and on-line services to disclose their policies concerning tracking of consumers' on-line activities and (ii) expand the scope of California's data breach notification law to include email addresses and login credentials that, in combination, could allow access to on-line accounts. A few days earlier, the Governor approved a law (iii) restricting the ability of commercial websites, on-line services, and on-line and mobile applications to advertise to children; to use, disclose, or compile minors' personal information; or to allow others to do so. Still awaiting the governor's signature or veto is a bill that would (iv) require warrants for state law enforcement agencies to gain access to virtually all stored electronic communications, thus going beyond its federal equivalent, the Stored Communications Act, in a way that some have been pushing for the federal law to be revised.

"Do Not Track"

California's "do not track" law is the first statute in the United States directly addressing websites' and on-line services' policies concerning tracking of consumers' on-line activities. The law, known as A.B. 370 as it moved through the legislature, amends the California Online Privacy Protection Act ("CalOPPA") to require operators of commercial websites and on-line services that collect personally identifiable information ("PII") about visitors to the sites or services to make two additional disclosures concerning their privacy policies:

- (i) "how the operator responds to Web browser 'do not track' signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of [PII] about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection"; and
- (ii) "whether other parties may collect [PII] about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service."[1]

The law provides that website and on-line service operators may satisfy the first of these obligations by "providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice." The law is limited to mandating additional disclosures and does not mandate any particular policies concerning "do not track" requests or activities.

CalOPPA had already required operators of commercial websites and on-line services that collect PII about visitors to post conspicuously or make available in other specified ways their privacy policies, including (i) the categories of PII they collect and the categories of third parties with whom they share that PII; (ii) the process (if any) by which visitors could request their collected PII and correct errors; (iii) the process by which they notify consumers of updates to the policy; and (iv) the policy's effective date.[2] Earlier versions of A.B. 370 would have imposed direct requirements on websites' and on-line services' tracking policies. The bill was amended in the course of the legislative process to limit it to disclosure obligations.

The law follows in the wake of a recommendation by the Federal Trade Commission ("FTC") that companies create mechanisms "to allow consumers to control the collection and use of their online browsing data," which, as the FTC has noted, has led to substantial industry efforts.[3] It also reflects the expanded on-line privacy enforcement efforts of California Attorney General Kamala Harris, who pushed for adoption of the "do not track" legislation. Efforts by the World Wide Web consortium to develop universal mechanisms for "expressing user preferences around Web tracking and for blocking or allowing Web tracking elements" have stumbled but continue to move forward.[4] Proposals for federal "do not track" legislation have not advanced far. Whether the California statute revives federal efforts remains to be seen. But in the meantime, all companies that operate websites or other on-line services that collect PII from California residents should review their privacy policies to ensure compliance with the new California law.

Data Breach Notification

The second law signed by Governor Brown on Friday amends California's data breach notification law to add as a category of covered PII "a user name or email address, in combination with a password or security question and answer that would permit access to an online account." The law allows the required notification of affected individuals in the case of breaches involving only this sort of information to direct the person promptly to change his or her password and security question or answer or to take other steps appropriate to protect the affected online account.[5]

California law already included in the definition of PII a person's first name or first initial and last name in combination with any of the following: (i) Social Security number, (ii) driver's license number, (iii) California ID card number, (iv) "[a]ccount number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account," (v) medical information, or (vi) health insurance information.[6] Efforts to establish federal data breach notification standards are again being pursued in the current Congress, but the proposed legislation seems unlikely to move forward at present.[7]

On-Line Privacy for Minors

On September 23, Governor Brown signed into law the Privacy Rights for Minors in a Digital World Act, enacted as S.B. 568, which:

- (i) prohibits operators of websites, online services, online applications, or mobile applications from marketing or advertising specified types of products or services to minors;
- (ii) prohibits operators from knowingly using, disclosing, compiling, or allowing a third-party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising specified types of products or services;
- (iii) makes this prohibition applicable to advertising services that are notified by an operator that the website, service, or application is directed to a minor;
- (iv) requires operators to permit a minor, who is a registered user of the operator's site, service, or application, to remove, or to request and obtain removal of, content or information posted on the site, service, or application by the minor (unless the content or information was posted by a third party, any other provision of state or federal law requires the operator or third party to maintain the content or information, or the operator anonymizes the content or information); and
- (v) requires operators to provide notice to minors that the minor may remove the content or information.[8]

The law takes effect on January 1, 2015.

The law's inclusion of mobile applications is noteworthy, particularly given the California Attorney General's aggressive enforcement efforts on mobile application privacy and security.[9]

Search Warrants for Stored Communications Such as Received Emails

The final bill in the group, still awaiting signature or veto by the governor, is S.B. 467, which would:

- (i) require law enforcement or other state agencies to get a warrant in order to gain access to any electronic communications held by providers of electronic communications services or remote computing services;
- (ii) require the agency to notify the affected customer of the warrant within three days, unless the agency could show that doing so may put someone's life or safety in danger, or may lead to destruction of evidence, a flight from prosecution, or intimidation of a potential witness;
- (iii) prohibit providers of electronic communications services or remote computing services from divulging the contents of stored electronic communications except in circumstances paralleling those in which disclosure is permitted under the federal Stored Communications Act[10]; and
- (iv) authorize civil causes of action for damage by parties harmed by violations of the law.[11]

Several features of the law are particularly noteworthy. First, unlike the federal Stored Communications Act, which requires a warrant only for communications held for 180 days or less, the California law establishes a warrant requirement regardless of the duration of storage.[12] Second, unlike the federal Act, which prohibits the divulging of communications only by providers of electronic communications services or remote computing services *to the public*, the California law extends its prohibition to all providers of those services.[13] It thus may apply to more companies than does its federal equivalent, though its exact scope will depend on judicial clarification.

---

[1] The text of the law, legislative history materials, and a comparison to prior law may be found here: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370. It is codified in section 22575(b)(5)-(7) of the California Business and Professions Code.

[2] *See* Cal. Bus. & Professions Code § 22575(a)(1)-(4).

[3] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers, at 4 (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[4] The work of the World Wide Web Consortium's Tracking Protection Group can be followed here: http://www.w3.org/2011/tracking-protection/.

[5] The text of the law, legislative history materials, and a comparison to prior law may be found here: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB46. It is codified in sections 1798.29 and 1798.82 of the California Civil Code.

[6] Cal. Civil Code § 1782(g).

[7] Senator Pat Toomey (R-PA) has introduced a federal data breach notification bill, which would include as a form of PII "[f]inancial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account." S. 1193, § 5(5), which is available here: http://www.gpo.gov/fdsys/pkg/BILLS-113s1193is/pdf/BILLS-113s1193is.pdf. Representative Marsha Blackburn (R-TN) has introduced a more general cybersecurity bill in the House, title 5 of which parallels Senator Toomey's breach notification bill. The House bill, H.R. 1468, is available here: http://www.gpo.gov/fdsys/pkg/BILLS-113hr1468ih/pdf/BILLS-113hr1468ih.pdf. Both bills have been referred to relevant committees.

[8] The text of the law, legislative history materials, and a comparison to prior law may be found here: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568. It is codified in sections 22580-22582 of the California Business and Professions Code.

[9] For a description of some of those efforts, see this post at our FinTech blog: http://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=10737418464#MobileApps.

[10] *See* 18 U.S.C. § 2702(b).

[11] The text of the law, legislative history materials, and a comparison to prior law may be found here: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB467. It is codified in sections 1524.2-1524.7 of the Penal Code. It includes exceptions that largely parallel its federal counterpart.

[12] *See* 18 U.S.C. § 2703(a)-(b).

[13] *See* 18 U.S.C. § 2702(a).