Computer Law Reporter

A MONTHLY JOURNAL OF COMPUTER LAW AND PRACTICE

Publisher:
Neil J. Cohen, Esq.

Volume 60, Number 6 | Washington, D.C. | February 2015

HIGHLIGHTS

The most noteworthy decisions this month are the following:

• In *Locklear v. Dow Jones & Company, Inc*., No. l:14-CV-00744-MHC (N.D. Ga. Jan. 23, 2015) plaintiff filed this class action alleging that Dow Jones & Company, Inc. violated the Video Privacy Protection Act (VPPA) by sharing personally identifiable information (PII) with mDialog, a third party, without consent. The Court held that Plaintiff had standing and qualified as a "consumer" under the VPPA. However, the Court held that the information that was shared was not PII because although mDialog was able to identify Plaintiff, mDialog had to take further steps (i.e., tum to sources other than Dow Jones) to match the information shared by Dow Jones to Plaintiff.

• In *Pascal Pour Elle, Ltd. v. Jin*, No. 1:14-cv-07943 (N.D. Ill. Dec. 9, 2014), in a case where a Salon's customer records were hacked by a former employee, the U.S. District Court for the Northern District of Illinois held that because the company's online management software program provided customers the ability to send or receive emails and text messages plaintiff adequately plead that it was an electronic communication service provider for purposes of stating a Stored Communications Act claim.

• In *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC* No. 14-3002 (6th Cir. Dec. 22, 2014), plaintiff's cost of a damages assessment after the unauthorized access of an online auction by false bidders constituted damages and loss under the Computer Fraud and Abuse Act, notwithstanding whether there was a "loss of service." Because the statute's definition of loss is sufficiently broad to

(continued on page 574)

Contents

Subscription price $3675 for one year. Published monthly by Computer Law Reporter, Inc., 1601 Connecticut Avenue, N.W., Suite 701, Washington, D.C. 20009 • Tel: 202-462-5755 • Fax: 202-328-2430 • ISSN: 0739-7771 • Publications Director: John G. Herring. Production Manager: Kristina M. Reznikov.

Computer Law Reporter
1601 Connecticut Avenue, N.W., Suite 701, Washington, D.C. 20009 • 202-462-5755 • Fax 202-328-2430

A Fresh Crop of California Data Privacy Laws

Lei Shen & Julian M. Dibbell*

California recently enacted three bills that expand the state's online privacy and data security laws. The changes include an expansion of California's existing data breach law, protections for the personal data of K-12 students and a new law giving minors a limited "right to be forgotten" in the online realm. Companies that handle the personal data of California residents, or that otherwise do business in the state, may find themselves affected by these new regulations in a variety of ways. The following summaries present a glimpse of the laws' key provisions and possible consequences.

A.B. 1710: Amended Law Widens Requirements for Data Breach Notification and Other Security Measures

Signed into law on September 30, 2014, and effective January 1, 2015, A.B. 1710 expands the reach of California's data breach notification law.[1] The amendments include (i) a requirement that identity theft protection services, if any, be offered free of charge for at least 12 months to California residents affected by a data breach; (ii) a broadening of "reasonable security" requirements to apply not only to businesses that own or license personal information but also to third parties with whom they share that information; and (iii) a ban on selling, advertising for sale or offering to sell any individual's Social Security number (SSN).

Free Identity Theft Protection Services in Some Cases of Data Breach

California law did not previously require a business to offer credit monitoring or other identity theft protection services to individuals affected by a data breach. A.B. 1710 amends the law so that if a business is the source of a data breach affecting a California resident, then "an offer to provide appropriate identity theft prevention and mitigation services, *if any*, shall be provided at no cost to the affected person for not less than 12 months [emphasis added]." The language is clear up to a point: there are now some circumstances under which the law requires businesses to provide identity theft protection free of charge and for at least one year. Exactly what those circumstances are, however, has been a much-debated question.

The question turns on the ambiguous limitation that the phrase "if any" places on the requirement. Some commentators read the limitation narrowly, interpreting the law to require free identity theft protection services if any such services are appropriate after a data breach, as in many cases they would be. Other commentators see a stronger limitation. For them, the law requires only that if any offer of identity theft protection services is made, then business choosing to make that offer must provide such services for free and for at least 12 months.

If this second interpretation is correct, then the law does little more than ratify the status quo, under which the voluntary offer of a year of free credit monitoring is already typical for some businesses' responses to data breach. If the first interpretation is correct, however, then the offer is no longer voluntary, and California becomes the first state to mandate the provision of identity theft protection in cases of data security breach. Unfortunately, neither reading is the clear winner, but look to California courts—or the state's attorney general—to make the call in time.

Security Requirements for Third-Party Recipients of Personal Information

Previously, the California data breach law required all businesses that *owned* or *licensed* personal information about a California resident to follow "reasonable security procedures and practices" designed to protect that information from "unauthorized access, destruction, use, modification, or disclosure." Where those businesses shared personal information with third parties, the law additionally

*Lei Shen and Julian M. Dibbell are associates in the Privacy & Security group at Mayer Brown in Chicago, IL. This article originally appeared on Mayer Brown's website. Reprinted by permission.

[1] Cal. Civ. Code § 1798.80 *et seq.*

obliged them to impose the same security requirements on their contracts with those third parties. As amended by A.B. 1710, the law now places its security requirements directly on third parties, adding businesses that neither own nor license but *maintain* personal information to the ranks of those that must adhere to the statute's reasonable security standard.

Prohibition on the Sale of Social Security Numbers

California law already prohibited businesses from publicly displaying any individual's SSN. A.B. 1710 expands that protection with a ban on "sell[ing], advertis[ing] for sale, or offer[ing] to sell" any individual's SSN. It also prohibits, even in the absence of a sale, the release of an SSN "for marketing purposes." Despite the ban, however, businesses may still release SSNs under a range of exceptions, including when doing so is "incidental to a larger transaction and necessary to a legitimate purpose" (as part of the sale of a company, for example), when it is specifically authorized by state or federal law and when it is for internal verification or administrative purposes.

S.B. 1177 (Student Online Personal Information Protection Act): New Law Targets Use of Student Data by Online Educational Services

When the Student Online Personal Information Protection Act (SOPIPA) was enacted on September 29, 2014, it entered a crowded field: 19 other states and the federal government have also passed laws protecting the personal data of students, most within the last year. Yet commentators have singled out SOPIPA as the nation's "first truly comprehensive student-data-privacy legislation."[2]

The law applies to online services designed and marketed for K-12 school purposes, and it places a broad range of obligations on those services. With some exceptions for legitimate educational and analytic purposes, the law prohibits covered services from engaging in targeted advertising to California students or their parents, from using personal information to create a profile of a student and from selling or otherwise disclosing a student's information. The law also requires a covered service to implement reasonable and appropriate security measures and to delete student records as requested by the student's school or district.

[2] http://blogs.edweek.org/edweek/DigitalEducation/2014/09/_landmark_student-data-privacy.html

A particularly distinctive feature of SOPIPA, relative to other student privacy laws, is its power to directly regulate the burgeoning educational-technology (or ed-tech) industry. The federal Family Educational Rights and Privacy Act (FERPA) and several of the state student privacy laws are focused on the governance of schools and school systems. SOPIPA, in contrast, imposes direct liability on ed-tech providers. Moreover, because the law implicitly creates broad public and private rights of action under California's Unfair Competition Law,[3] enforcement is likely to be more frequent and more nimble than the US Department of Education's FERPA enforcement actions.

SOPIPA takes effect on January 1, 2016. Given the breadth of the law's provisions and its robust prospects for enforcement, businesses providing online services that could be deemed educational should, prior to that date, determine whether SOPIPA applies to them.

S.B 568 (Privacy Rights for California Minors in the Digital World): New Law Gives Minors a Narrow "Right To Be Forgotten" and Limits Online Marketing Aimed at Them

In yet another California data-privacy first, S.B. 568, enacted September 23, 2013, and effective January 1, 2015, makes California the first state to pass a law providing Internet users under 18 a right to delete or otherwise remove content they have posted online. In addition, the law prohibits online sites from marketing to minors goods and services not legally available to them, including alcohol, tobacco, tattoos and tanning salons.

The content-removal provision has been widely referred to as a "right to be forgotten" for minors. However, compared to the broadly enforceable "right to be forgotten" recently adopted by the European Union, the California law is extremely limited in reach. The law requires online sites to permit a registered user who is a California minor to remove from view any content that the minor has posted on the site, and to provide notice to all such minors of the option to remove their content and the steps required to do so. Notably, the law exempts from its requirements any content that was posted by a third party other than the minor, even if that content reposts the minor's original post. Other

[3] Cal. Bus. & Prof. Code §§ 17200-17209.

exemptions include content posted by a minor in exchange for compensation, anonymized content, and content that any other provision of state or federal law prohibits the site from removing.

The law also prohibits sites "directed to minors" from advertising any of a long list of products banned for sale to minors in California (though not necessarily in other jurisdictions). It also prohibits general-audience sites from knowingly targeting minors with ads for those products. Online businesses that can afford to cut out ads from, for example, the alcohol and tobacco industries, may want to do so if their existing content has appeal to people under the age of eighteen. Others may find it more cost-effective to ban minors from their sites entirely.

Conclusion

California has long been a pioneer in the regulation of online privacy. For businesses that operate in the state or process its residents' personal information, keeping up with California's frequent innovations in the field is vital.

