New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 262—NO. 103
TUESDAY, NOVEMBER 26, 2019

Outside Counsel

Expert Analysis

Experimentation in Privacy Law Leads to Increased Complexity

By **Paul Greene**

It has always been a "happy incident" of our federal system that a "courageous State" may "try novel social and economic experiments without risk to the rest of the country." See *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J. dissenting). In relation to data protection laws, however, this has led to an unintended and potentially unworkable level of complexity on the national level. This complexity first arose in relation to data breach notification statutes, which began in California in 2002 and soon spread to all 50 states, albeit with wide variations in terminology and scope.

In relation to data privacy, California is again leading the way with the California Consumer Privacy Act (CCPA), passed in 2018 and effective as of Jan. 1, 2020. Long gone are the days, however, where experimentation in the arena of data protection is "without risk to the rest of the country." Indeed, as the world's fifth largest economy and nexus for much of the world's commercial online activity, California has global weight when it comes to regulating how organizations process personal data. This weight was underscored recently with the release of proposed regulations under CCPA, which remain under comment until Dec. 6, 2019.

The proposed regulations fill certain gaps in the statutory language of CCPA and arguably extend CCPA into areas not directly addressed by the Act. This type of administrative "creep" is another, perhaps not so "happy incident" of our federal system: Administrative agencies tasked with creating regulations can themselves be a form of laboratory where the "experiments" of democracy take place. And adding to the complexity facing organizations before the effective date of CCPA are the jurisdictions following California's lead, considering their own, customized versions of CCPA, as well as other jurisdictions considering novel privacy regimes of their own.

Despite this complexity, certain similarities appear, such as the right to opt out of sale of one's personal data and obligatory privacy disclosures for businesses that collect such data. Compare Cal. Civ. Code §1798.120 (CCPA "right to opt out" provision), with S.B. 220, 80th Sess. (Nev. 2019)

As the world's fifth largest economy and nexus for much of the world's commercial online activity, California has global weight when it comes to regulating how organizations process personal data.

F. PAUL GREENE *is a partner and chair of the privacy and data security practice group at Harter Secrest & Emery, a full-service business law firm with offices throughout New York. He can be reached at fgreene@hselaw.com.*

(to be codified at Nev. Rev. Stat. ch. 603A) (Nevada right to opt out). Differences abound, however, making the data protection journey more difficult for organizations with connections to multiple state jurisdictions.

Chief among these differences is how states deal with the issue of pre-existing privacy obligations under federal or state law. California, for example, has exempted from CCPA "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act" (GLBA), as well as any "protected health information that is collected by a covered entity or business associate governed by [...] the Health Insurance Portability and Accountability Act" (HIPAA) and "the Health Information Technology for Economic and Clinical Health Act" (HITECH). See Cal. Civ. Code. §1798.145(e), (c)(1)(A). In doing this, California has adopted a data-driven exemption to CCPA, rather than an entity-driven one, exempting entities insofar as they process data regulated under GLBA or HIPAA/HITECH. This data-driven approach can lead to the circumstance, however, where a consumer-facing bank enjoys an exemption from CCPA in relation to consumer data, but not in relation to data collected from employees or in commercial banking activities. Perhaps for this very reason, other jurisdictions, such as Nevada and New York, have taken more entity-driven approaches to their exemptions. Specifically, Nevada law exempts any "entity that is subject to" HIPAA from its new rules requiring privacy disclosures and opt-out procedures from defined "operators" of commercial websites targeting Nevadans, and certain security provisions of the NY SHIELD Act, which become effective in March 2020, exempt from their scope any "person or business that is subject to, and in compliance with" the security provisions of HIPAA and HITECH, for example. And others are considering doing away with these exemptions entirely, as can be seen in Pennsylvania House Bill 1049, a CCPA analog that omits any exemption for GLBA-related data processing or GLBA-regulated entities. H.B. 1049, Gen. Assemb., Reg. Sess. (Pa. 2019).

> Both CCPA and the proposed regulations may substantially restrict direct marketing based on discounts or promotional offers.

Another difference is the idea of "privacy by default," which was made part of the European Union's General Data Protection Regulation (GDPR) that took effect in May 2018, and has crept into some of the provisions found in the proposed CCPA regulations. Specifically, CCPA created provisions for "privacy by choice," e.g., the right to opt out of sale of personal information. The proposed CCPA regulations go further in two important respects. First, if a business collects personal information without providing a notice of the consumer's right to opt out, the business must treat the personal information collected as affirmatively opted out of sale. See California Consumer Privacy Act Regulations §999.306(d)(2) (proposed Oct. 11, 2019) (to be codified at 11 C.C.R. ch. 20) (Proposed CCPA Regulations). Second, if a business receives a consumer request to delete but cannot verify it, the business must treat it as a valid opt-out-of-sale request, despite the lack of verification. See id. §999.313(d)(1). It is only a small step from provisions such as these to a full-blown privacy by default approach, which would forbid any processing of personal information without either opt-in consent or other valid grounds for processing. See, e.g., GDPR Art. 6 (processing only lawful if conducted on consent or if other specific requirements met).

The proposed CCPA regulations also borrow from GDPR in relation to privacy notices, specifically requiring the use of "just-in-time" notices, which have been endorsed by the United Kingdom's Information Commissioner's Office in relation to GDPR-required notices. Where the statutory text of CCPA requires privacy notices "at or before the point of collection,"

the regulations add additional requirements in several important ways. First, they require a business make its disclosure "accessible where consumers will see it before any personal information is collected." See Proposed CCPA Regulations §999.305(a)(2)(e). Similarly, when disclosing a consumer's right to opt out of sale of the consumer's personal information, the proposed regulations require businesses that substantially interact with consumers offline to provide an offline method of notice, such as a paper notice or signage with appropriate disclosures. See id. §999.306(b)(2). And in relation to consumer requests to access their personal information held by a business, or to have the business delete information it has collected from the consumer, a business must consider the method by which it interacts with the consumer when determining how such requests should be submitted. Whereas CCPA requires only a toll-free number and a website address for submission of such requests, the proposed regulations can require, for example, a brick-and-mortar retailer to also provide a "form that can be submitted in person at the retail location." Compare Cal. Civ. Code. §1798.130(a)(1), with Proposed CCPA Regulations §999.312(c)(2).

And the proposed regulations take a business's duties in relation to consumer data requests a step further, requiring a business that receives such a request in a manner other than the one designated by the business to either treat the request as if it had been submitted appropriately or "[p]rovide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request." See Proposed CCPA Regulations §999.312(f)(2). This task, although simplistic at first glance, becomes herculean when considering large organizations with extensive consumer contact. In such organizations, effectively every employee will have to be able to direct a faulty consumer data request to the appropriate internal stakeholders, or provide specific directions to the consumer on how to submit the request correctly. It remains to be seen how public comment on this provision will shape it going forward.

Lastly, both CCPA and the proposed regulations may substantially restrict direct marketing based on discounts or promotional offers. CCPA includes a principle of non-discrimination, under which a business is prohibited from denying goods or services to a consumer, or charging different prices or providing a different level of quality of goods or services to a consumer, because a consumer, for example, exercises his or her right to deletion. See Cal. Civ. Code §1798.125(a)(1). The proposed regulations further clarify that if a retail store offers discounted prices to consumers that sign up to be on the store's mailing list, those discounts are only nondiscriminatory if the consumer can still obtain them after requesting that the store delete the consumer's address. See Proposed CCPA Regulations §999.336(c)(2). This, of course, calls into question how targeted offers can survive CCPA, if they can no longer be limited to those consumers that opt in to having a business maintain their contact information.

Public hearings will be held in relation to the proposed regulations in December, and the issues addressed above may well change in light of those hearings and public comment. The one constant, however, in relation to both CCPA and other privacy "experiments" underway in states around the country, is that the current level of complexity in relation to data protection laws will continue for the foreseeable future, and likely even increase, as CCPA analogs and other data protection regimes proliferate.