LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, NOVEMBER 9, 2020

PERSPECTIVE

Here comes a wave of data privacy litigation

By Gary Lincenberg, Steven Zipperstein and Darren Patrick

Data privacy law is quickly becoming the hottest legal issue of the 2020s. Over the previous decade — amid the rapid growth of tech giants like Google, Facebook, Twitter and Amazon — consumers gradually came to realize that their "personal" information was both a commodity and a building block in the expanding artificial intelligence infrastructure. Products we browsed crept into online ads. Google search results became geographically localized, then "predictively" finished our thoughts. Soon enough, our social media "feeds" reflected every dimension of our online lives. "Alexa" was listening in and — as Amazon recently confirmed — storing transcripts of our human-to-cyborg colloquies indefinitely. Meanwhile, privacy advocates decried that mobile apps could activate the microphones and cameras in our phones. In the pursuit of technological progress, had we unwittingly consented to being "watched"?

Data privacy is now a global concern, with an increasingly geopolitical twist. Center stage are concerns about foreign interference. Chinese social media platforms WeChat and TikTok monitor, store, and have been accused of intercepting "sensitive" political content. TikTok has allegedly recommended video content based in part on race and age information it gleans from users' digital face images. The Cambridge Analytica scandal illustrated how political groups worldwide have targeted social media users in an attempt to influence elections. The Mueller report detailed examples of this, such as Russian actors using Facebook ads to organize political demonstrations to help Trump's candidacy.

Against this backdrop, 2020 has seen three significant developments in data privacy law. In July, California Attorney General Xavier Becerra announced the imminent enforcement of the California Consumer Privacy Act of 2018, the most comprehensive consumer data privacy law in history. Simultaneously, in *Schrems II*, the European Court of Justice overturned the transatlantic "privacy shield" governing data transfers from Europe to the United States. On Nov. 3, California voters approved Proposition 24, which creates the California Privacy Rights and Enforcement Act of 2020. The CPRA amends the California Consumer Privacy Act to provide further protections for consumers' personal information. Within California, the CCPA and CPRA mandate extensive disclosure requirements and grant consumers unprecedented rights to "opt out" of large swaths of the data collection process. These developments highlight the need for businesses that collect personal data to implement comprehensive compliance protocols to protect against possible liability.

The CCPA

The CCPA became effective in July. On Aug. 14, the Office of Administrative Law approved the Department of Justice's governing regulations, which are now in effect. The CCPA applies to any for-profit business operating in California that: (i) has annual gross revenues in excess of $25 million; (ii) buys, sells, receives, or shares the personal information of 50,000 or more consumers, households, or devices annually; or (iii) derives 50% or more of its annual revenues from selling consumer's personal information. Civ. Code Section 1798.140(c).

"Personal information" is defined broadly to include any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.* Section 1798.140(o)(1). The statute contains a nonexclusive list of examples, including consumers' IP addresses, online identifiers, search terms, browsing histories, purchasing histories or "tendencies," interactions with advertisements, location data, audio and visual information, and biometric information. *Id.*

The CCPA creates four basic sets of data privacy rights and obligations:

• *Right To Know.* Businesses must inform consumers of the categories of personal information they collect, and the purposes for which it is used. Upon request, businesses must also notify consumers of the types of third parties it shares their personal information with, and deliver to consumers the personal information they have collected about them. *Id.* Section 1798.115.

• *Right to Opt-Out.* Businesses must allow consumers to "opt out" of having their personal information sold to third parties (e.g., advertisers or data brokers) and provide a "clear and conspicuous" link to their opt-out page. Section 1798.120. •

Right to Delete. Upon request, and subject to certain exceptions, business must delete consumers' personal data from their records. *Id.* Section 1798.105.

• *Right to Non-Discrimination.* Businesses cannot deny goods or services, charge consumers a different price, or provide a different level or quality of goods or services because they exercised their rights under the CCPA. *Id.* Section 1798.125. Regulations provide detailed guidance on the CCPA's notice requirements. For example, notices must be reasonably accessible to persons with disabilities. Code Regs., tit. 20, Section 999.305(a)(2)(d). Businesses must also post a privacy policy — "through a conspicuous link" on their website homepage or mobile application — including a "comprehensive description" of their data collection practices. *Id.* Sections 999.305(a)(1), (a)(3)(a). Further, the regulations make clear that the CCPA does not apply only to online data collection: if businesses collect personal information over the telephone or in person, they must provide the required notices orally. *Id.* Section 999.305(a)(3)(d).

Special Protections for Minors

Under the CCPA, business are prohibited from selling the personal information of consumers under 16 years of age unless the consumer (if at least 13 years old) "opts in" by affirmatively authorizing such a sale. For consumers under 13, a parent or guardian must provide the "optin" authorization. Civ. Code Section 1798.120(c). Under the applicable regulations, a business that has actual knowledge that it sells the personal information of a consumer under the age of 13 must establish, document, and adopt a "reasonable method" for determining that the person affirmatively authorizing the sale of the personal information about the child is, in fact, the parent or guardian of that child — including by the use of consent forms signed under penalty of perjury and the verification of the guardian's government issued ID. Code Regs., tit. 20, Section 999.330(a). When receiving a request to "opt-in" from a minor or guardian, a business must also give notice of the right to optout a later time, *unless* that business exclusively targets goods and services to consumers under 16. *Id.* Section 999.332(b).

Enforcement

The principal power to enforce the CCPA, as originally enacted, lies with the California attorney general. After providing a business with a notice of noncompliance and a 30-day opportunity to cure the noncompliance, the AG is authorized to bring actions for injunctive relief and civil penalties: $2,500 per violation and $7,500 for each intentional violation. Cal. Civ. Code Section 1798.155(b).

By contrast, consumer remedies under the CCPA are limited in several key respects. Consumers can sue businesses only if their non-encrypted and non-redacted personal information was stolen in a data breach as a result of the business' failure to maintain reasonable security procedures and practices to protect it. *Id.* Section 1798.150(a)(1). Further, the broad definition of "personal information" contained in the CCPA — which encompasses virtually all information created or shared on the internet — does not apply for purposes of consumer actions. Such actions can be based only on breaches of specific types of personal information, as that term is defined in California's 20-year old data breach notification statute. *Id.* There, "personal information" means only individuals' names in combination with their (i) social security or other government issued ID number; (ii) bank account numbers (but only if combined with a code or password that would permit access to the account); (iii) medical or health insurance information; or (iv) biometric data. *Id.* Section 1798.81.5. In such cases, a consumer may initiate — subject to a 30 day notice and cure period — a civil action for statutory damages ($100- $750 per consumer per incident) or actual damages, whichever is greater, as well as injunctive relief. *Id.* Section 1798.150(a)(1).

The CPRA

The principal provisions of the California Privacy Rights and Enforcement Act become effective on January 1, 2023. The Act expands the CCPA in several key areas:

• *New Enforcement Agency.* The CPRA creates the California Privacy Protection Agency, the first state agency dedicated to privacy enforcement. Civ. Code Section 1798.199.10 et seq. The agency — to be governed by a five-member board appointed by the governor, attorney general, Senate Rules Committee, and speaker of the Assembly —– will be vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. *Id.* However, at the request of the attorney general, the agency must stay an investigation or civil action, and may proceed only if the AG elects not to pursue a claim. *See id.* Section 1798.199.90(c) (further providing that the "Agency may not limit the authority of the attorney general to enforce this title"). On the other hand, the authority to issue regulations will pass from the attorney general to the agency "[b]eginning the later of July 1, 2021, or six months after the agency provides notice to the attorney general that it is prepared to begin rulemaking under this title." *Id.* Section 1798.185(d). Similar to the civil penalties available in an action by the attorney general, the agency is authorized (but not required) to levy administrative fines of up to $2,500 for each violation, or up to $7,500 for each intentional violation or violation involving the personal information of minor consumers. *Id.* Section 1798.199.55(a)(2).

• *"Sensitive" Information.* The CPRA adds a new layer of protection for "sensitive personal information," which includes government- issued identifiers, log-in information, financial information, precise geolocation, race or ethnic origin, religious beliefs, genetic data, biometric information, and sexual orientation, as well as the content of mail, email, and text messages. *Id.* Section 1798.140(ae). Under the CPRA, consumers may direct a business to limit its use or disclosure of sensitive personal information to what is "necessary to perform the services or provide goods reasonably expected by an average consumer," or to perform certain other designated services. *Id.* Section 1798.121. The CPRA also includes special notice requirements regarding sensitive information, and requires businesses to add a "Limit the Use of My Sensitive Personal Information" link on their websites. *Id.* Section 1798.135(a) (2).

• *"Sharing" Information.* Under the CPRA, a business' *sharing* personal information is subject to the same notice requirements (and opt-out rights) as a business' *selling* personal information. *Id.* Section 1798.120. Businesses must also include a "Do Not Sell or Share My Personal Information" link on their websites. *Id.* Section 1798.135(a) (1).

• *Expanded Private Actions.* As noted above, the CCPA's private right of action only applies in the event of a breach of non-encrypted and non-redacted personal information, as narrowly defined by California's data breach statute. The CPRA adds email addresses, when combined with a password (or equivalent) that would permit access to an account, to the definition of "personal information" for purposes of private suits. *Id.* Section 1798.150(a)(1). Additionally, regarding the 30-day cure period for private actions, the CPRA clarifies that the "implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach." *Id.* Section 1798.150(C)(2)(b).

At the same time, the CPRA builds in higher thresholds for the definition of "business," which should result in fewer small businesses falling within the scope of the CPRA. *Id.* Section 1798.140(d)(1)(B). The CPRA also extends the CCPA's exemptions for information relating to employees, job applicants and business-to-business contacts until Jan. 1, 2023.

Schrems II Decision

The third major data privacy development of 2020 comes out of Europe. In what is referred to as the *Schrems II* decision, the European Court of Justice overturned the "EU- US Privacy Shield" system which had governed data transfers from Europe to the United States since 2016. *See Data Protection Commissioner v. Facebook & Max Schrems*, CJEU Case C-311/18. In so doing, the ECJ effectively reinstated the baseline protections of the European General Data Protection Regulation, which is even more protective of personal information than the CCPA.

The GDPR originated in a 1995 directive of the European Parliament. It generally prohibits cross-border transfers of data unless (1) the European Commission has granted the recipient country an "adequacy decision"; (2) the controller or processor of the data provides "appropriate safeguards"; or (3) the cross-border data transfer is justified under one of the enumerated "derogations" (or exceptions). *See* GDPR Arts. 45, 46, 49; Directive 95/46/EC, OJ 1995 L 281, p. 31 et seq. ("Directive"). The principal "derogation" is the subject's "unambiguous consent" to the data transfer. *See* Directive Art. 26 ¶ 1; GDPR Art. 45.

In 2000, side-stepping the "unambiguous consent" requirement, the European Commission approved as "adequate" the "Safe Harbor" regime proposed by the U.S. Secretary of Commerce for E.U.-U.S. data transfers. *See* Decision 2000/520/ EC, OJ 2000 L 215, p. 7 et seq."). The Safe Harbor rules required (1) notice to users and (2) the ability of users to "opt out" of data collection. *See* OJ 2000 L 215, Annex I (the "Safe Harbor Principles"). Reminiscent of the CCPA's protections, the Safe Harbor Principles provided, for example, that an "organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure." *Id.* at 12. The principles also specified that the required notice "must be provided in clear and conspicuous language … before the organization uses such information for a purpose other than that for which it was originally collected or processed." *Id.* However, in its 2015 *Schrems I* ruling, the ECJ overruled the "Safe Harbor" regime "in light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services." *See Maximillian Schrems v. Data Protection Commissioner*, CJEU Case C 362/14.

In 2016, the European Commission responded to Schrems I by passing the "EU-US Privacy Shield," whose main features included (1) "assurance" from the U.S. that the "access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms"; and (2) the institution of an "ombudsperson" mechanism to address complaints regarding data privacy breaches. But in the 2020 *Schrems II* decision, the ECJ invalidated the "EUUS Privacy Shield," again on the grounds that federal agencies (like the NSA) can collect personal data stored within the U.S. with little to no oversight.

As the ECJ decision appears to concede, the specter of large-scale government surveillance is outside the control of foreign governments, much less businesses that collect personal data from consumers. Indeed, implicit in the *Schrems II* decision is that businesses could never provide the "appropriate safeguards" over personal information contemplated by the GDPR. *See* GDPR Art. 46. On the other hand, businesses (including those outside California) could go a long way towards satisfying the "unambiguous consent" derogation by implementing the requirements of the CCPA and CPRA.

Takeaways

California has the fifth largest economy in the world. As such, businesses ignore at their peril the state's new data privacy laws. Businesses should be acting now to ensure compliance with the CCPA and CPRA. Expect to see the state attorney general ramp up its enforcement branch. Expect to see plaintiff class action firms figure out ways to combine the new statutes with the Business and Professions Code and other statutes to allow private actors to bring broad consumer claims under state law. Given the drumbeat of political attacks on tech giants, and newly legislated weapons, expect data privacy to be a hotbed of litigation over the next decade. ■

Gary Lincenberg, Steven Zipperstein *and* **Darren Patrick** *are with the firm Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C.*