Insert for SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW

To be inserted in Chapter 9 at p.918. Part F -- Statutory Regulation will become Part F – Federal Statutory Regulation. A new Part G will be added called State Statutory Regulation. Existing Part G – First Amendment Limitations on Privacy Regulation will be Part H.

G. STATE STATUTORY REGULATION

1. CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act (CCPA) was passed in 2018. The CCPA provides for many consumer privacy rights. It imposes many responsibilities on companies that collect and use personal data. The CCPA is one of the strongest state privacy laws in the United States. It also goes far beyond many federal laws.

This law was hurried through the legislative process to avoid a proposed ballot initiative with the same name. The ballot initiative was the creation of Alastair Mactaggart, a real estate developer who spent millions to bring the initiative to the ballot. Mactaggart indicated that he would withdraw the initiative if the legislature were to pass a similar law, and this is what prompted the rush to pass the new Act, as the deadline to withdraw the initiative was looming. The CCPA took effect on January 1, 2020, but much about the law remains uncertain. In October 2019, Xavier Becerra, the Attorney General of California, released a draft of proposed regulations for the law. The expected date for final regulations is July 2020.

Scope and Applicability. The CCPA applies to all for-profit companies that collect and maintain personal data from California residents, do business in the state, and: (a) have annual gross revenues exceeding $25 million, or (b) obtain the personal information of 50,000 or more California residents, households, or devices on annually, or (c) derive 50 percent or more of their annual revenues from selling California residents' personal information. Except with respect to unauthorized theft and disclosure of information, the Act does not apply to banks, brokerages, insurance companies, and credit reporting agencies regulated under federal law. The CCPA also exempts certain activities relating to medical information, such as data collected as part of clinical trials.

Definition of Personal Information. The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

Consumer Rights. The CCPA provides for a number of consumer rights, including:

- Right to be notified about information collected and the purpose of use
- Right of consumers to request and receive disclosures about their personal information within the past 12 months
- Right to data portability
- Right to have businesses and their service providers delete their personal information
- Right to opt out of the sale of personal information to third parties
- Right to opt-in for children's personal information

Notice. The CCPA requires companies to notify consumers about the existence and nature of their rights, the categories of personal information collected, the purposes for which that personal information is collected, and the categories of personal information that companies disclose. Notice may be provided in a company's privacy policy or at the time the personal data is collected.

Right to Request and Receive Disclosures. Consumers have the right to know the sources from which a company collected the consumer's personal information, categories of information collected, and the third parties with which it shared that information. Consumers have the right to request the specific pieces of personal information collected about them.

The request must be a "verified" request, as the business must be able to verify that the person requesting the disclosures is the actual individual authorized to receive the information. Businesses must provide two or more ways for consumers to request information. According to the Attorney General's Draft Regulations, businesses are to respond to these requests within forty-five days. If the business provides the consumer "with notice and explanation of the reason that the business will take more than 45 days to respond to the request[,]" the business may have another 45 days to respond to the request. Draft Regulations, § 999.313(b).

Right to Deletion. A "business that receives a verifiable request from a consumer to delete the consumer's personal information . . . shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records." Exceptions to the right of deletion include necessary business operations such as the need to perform contracts with the consumer. Personal information does not need to be deleted when a company is engaging in "internal" uses that are "reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" and when the information is used "in a lawful manner that is compatible with the context in which the consumer provided the information."

Right to Opt Out. The CCPA provides consumers with a right to opt out of the sale of personal information to third parties. According to the CCPA, a "sale" of personal information means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

Prohibition on Denial of Goods or Services for Exercising Privacy Rights. Companies cannot discriminate against consumers by denying goods or services or charging different prices to consumers who exercise their privacy rights under the Act. However, a company may do so "if that difference is reasonably related to the value provided to the consumer by the consumer's data." Companies are allowed to "offer financial incentives, including payments to consumers as compensation," for collecting and selling their personal information.

Enforcement. The CCPA will be enforced by the California Attorney General. Civil penalties for intentional violation of the Act can be up to $7,500 per violation.

Private Right of Action for Data Breaches. Although the CCPA lacks a private right of action for most violations, it creates a private right of action in the event of "unauthorized access and exfiltration, theft, or disclosure" of a consumer's nonencrypted or nonredacted personal information. Before bringing an action, consumers must provide written notice to the business identifying the specific provisions allegedly being violated. If the business "cures" the violations and provides a written statement to the consumer attesting to this fact within 30 days, however, then no action for statutory damages can be taken against the business. The CCPA restricts its "cure" provision, moreover, by limiting it to circumstances under which "a cure is possible." It also creates other restrictions on an entity's ability to claim this safe harbor. In its relevant section, the CCPA provides:

> In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.

Thus, there is considerable ambiguity in the CCPA regarding what it means to "cure" a data breach. The Attorney General's Draft Regulations do not provide any clarification of this language.

The CCPA does not require written notice prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations. Recovery of damages can be "not more than $2,500 per violation or $7,500 per each intentional violation." Further, an injunction is also available as a remedy. Contrary to previous versions of the Act, the California Attorney General may not intervene in private lawsuits.

NOTES & QUESTIONS

1. ***Scope and Applicability of the CCPA.*** The CCPA only applies to "businesses," which are for-profit companies. Other types of organizations, such as non-profit or government entities, are not covered. Should the CCPA apply to government? Non-profits?

The CCPA also aims to apply to businesses of a particular size by including thresholds for revenue or number of California residents. In contrast, other laws such as the EU's General Data Protection Regulation (GDPR) apply to businesses of any size. What are the pros and cons of including business size thresholds to trigger privacy regulation?

2. ***Definition of Personal Information.*** The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This definition is similar to the GDPR's definition of "personal data" in that it includes information that is *identifiable* — that could be linked directly or indirectly to people. But it diverges in that it excludes "publicly available information" — "information that is lawfully made available from federal, state, or local government records." The definition also diverges from the GDPR and most other privacy laws in that it includes information identifiable to a household, not just a particular individual. What are the implications of making household information "personal information" under the CCPA?
3. ***Verified Requests for Disclosures.*** A big challenge with the CCPA is how to verify that the person requesting disclosures of their personal information is indeed the person authorized to receive the disclosures. The CCPA states that consumers must be able to make verified requests for their personal information without having to have an account or to create an account. Many businesses collect data based on IP addresses or cookies, and they don't know more about the identity of these people. How are people to be verified if businesses don't have an account for that person or even their name or contact information?
4. ***"Curing" a Data Breach?*** What does it mean for a business to "cure" a data breach? Does it mean that the entity has changed the practices that lead to the leak of the data? Does it mean that it has repaired any harm to the consumer? Another set of issues relates to the necessary representation that "no further violations shall occur." If there is a further data breach, can this representation create liability for a business?
5. ***Privacy Self-Management.*** The CCPA is primarily a "privacy self-management" law – to use the terminology of Daniel Solove. The CCPA allows people to find out the data that companies are gathering about them as well as allows people to opt out of the sale of their data. According to Solove, however, relying on people to manage their own privacy is not likely to provide meaningful protection because many people cannot understand the full costs and benefits of making various decisions about their data. If it isn't enough to provide people with information about the data being gathered about them and to give them a right to opt out, what else can be done to protect privacy? If the CCPA is not effective enough, what could strengthen it?

2. BIOMETRIC PRIVACY LAWS

(a) Illinois Biometric Information Privacy Act

The Biometric Information Protection Act (BIPA), 740 ILCS 14/1 *et seq.*, was passed by the Illinois legislature in 2008. The statute provides Illinois citizens with right regarding their biometric data.

Scope and Applicability. The BIPA applies only to "private entities," which includes both for-profit and non-profit organizations. State and local governmental agencies and courts are not covered.

Definition of Biometric Information. The BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers."

The definition of "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The Act then lists a series of things that are not to be deemed to be a biometric identifier: "Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color,"

The Act goes on to exclude donated body parts, blood, or tissues, "biological materials regulated under the Genetic Information Privacy Act," "information collected, used, or stored for health care treatment, payment, or operations" under HIPAA, or an "X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening."

Written Retention Policy. The BIPA requires private entities using biometric information to "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."

Written Individual Notice. In order to collect or obtain biometric information, private entities must first inform people "that a biometric identifier or biometric information is being collected or stored." This notice must be in writing. The notice must disclose the "specific purpose" and length of time for the collection, storage, and use of the biometric data. Private entities must receive a "written release" from people (or their representatives) in order to collect or obtain their biometric information.

Prohibition on Sale or Profit. Private entities are forbidden from selling or otherwise profiting from a person's biometric data.

Restrictions on Disclosure. The BIPA restricts the disclosure of biometric information unless "the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure." Other exceptions include where the disclosure is to complete a financial transaction authorized by the person or the disclosure is required by law or by a valid warrant or subpoena.

Enforcement. The BIPA is enforced by a private right of action: "Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." For negligent violations, the Act provides for "liquidated damages of $1,000 or actual damages, whichever is greater." For intentional or reckless violations, the BIPA provides for "liquidated damages of $5,000 or actual damages, whichever is greater." The BIAA also includes attorney's fees, costs, and injunctive relief.

(b) Other State Biometric Laws

Several other states followed Illinois in passing biometric privacy laws. Texas passed a biometric privacy law in 2009. The Texas law requires consent for the use or disclosure of biometric identifiers, but the consent does not have to be written. There is a prohibition on selling biometric identifiers except for limited purposes. Companies must destroy biometric identifiers withing a "reasonable time" after the data is no longer needed, and this period cannot exceed one year after the data is no longer necessary. Unlike the Illinois BIPA, the Texas law has no private right of action. The Texas law is enforced by the state attorney general who can fine up to $25,000 per violation.

In 2017, Washington enacted a biometric privacy law that requires companies to provide notice, obtain consent, and limit the purpose and use of biometric data. Similar to the Texas law, the Washington law does not require written consent and lacks a private right of action. Biometric information defined broadly as "data generated by automatic measurements of an individual's biological characteristics."

NOTES & QUESTIONS

1. ***An Application of the BIPA.*** Suppose the owner of a bar wants to use facial recognition technology to identify individuals who have been banned from the bar if they try to enter the bar again after being banned. Individuals are banned when they engage in dangerous or threatening conduct or harass other patrons. How would you advise the owner about the use of facial recognition technology for this purpose?
2. ***Harm and "Aggrieved" Persons.*** In *Rosenbach v. Six Flags Ent. Corp.,* 129 N.E.3d 1197 (Ill. 2019), Six Flags obtained Rosenbach's son's thumbprint for a seasonal pass. Six Flags failed to notify Rosenbach in writing of the intended

purpose and length of time for the use of the thumbprint, and it failed to obtain written consent.

Without asserting actual damages, Six Flags argued there was no standing to bring suit since there was no actual harm or injury to Rosenbach or her son. Six Flags further argued that Rosenbach was not an "aggrieved person" within the meaning of BIPA. The Illinois Supreme Court sided with Rosenbach:

> More than a century ago, our court held that to be aggrieved simply "means having a substantial grievance; a denial of some personal or property right. A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as "aggrieved." Rather, "[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of *or* his pecuniary interest is directly affected by the decree or judgment."

3. Spokeo *and Harm for BIPA Violations.* BIPA authorizes liquidated damages for all types of violations. In *Spokeo v. Robins*, the U.S. Supreme Court held that for standing in federal court, mere procedural violations of statutes that did not cause a concrete injury were not sufficient for standing despite the existence of statutory remedies. When BIPA actions are included in federal litigation (as opposed to state litigation), the requirements of standing must be met.

In *Patel v. Facebook Inc.*, 932 F.3d 1264 (9th Cir. 2019), Facebook users in Illinois brought a class action against Facebook, arguing Facebook's facial-recognition and "Tag Suggestions" program that collected and stored their facial geometry violated BIPA. Facebook failed to obtain written consent and failed to provide a compliant retention schedule. Facebook argued there was no injury in fact, and thus no standing, since data storage took place outside of Illinois.

In light of *Spokeo*, the court developed a test to determine whether a statutory violation causes a concrete injury: "We ask '(1) whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests.'"

As for the first part of the test, the court concluded:

> In light of this historical background and the Supreme Court's views regarding enhanced technological intrusions on the right to privacy, we conclude that an invasion of an individual's biometric privacy rights "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo.* "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." As in the Fourth Amendment context, the facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. *Carpenter.* Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present

> in the photo. Taking into account the future development of such technology as suggested in *Carpenter*, it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone. We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law.

Regarding the second part of the test, the court concluded that the provisions of the BIPA that were violated were not mere procedural violations:

> Facebook's alleged collection, use, and storage of plaintiffs' face templates here is the very substantive harm targeted by BIPA. Because we conclude that BIPA protects the plaintiffs' concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests, the plaintiffs have alleged a concrete and particularized harm, sufficient to confer Article III standing.

How does the court distinguish between mere procedural violations of the BIPA and substantive ones? Based on *Patel*, is anything a mere procedural violation of the BIPA?