3. Security breach litigation

By C. Kibby

Section 1798.150 of the California Consumer Privacy Act, as amended by the California Privacy Rights Act, provides a private right of action that allows private plaintiffs to bring civil actions against businesses in limited circumstances.

The CCPA is unique among its cohort of comprehensive state privacy laws for having a PRA. While every such law contains enforcement avenues for public authorities, such as attorneys general and government agencies, the CCPA is the only comprehensive state privacy law passed so far to include a PRA. Washington state's My Health My Data Act and Illinois' Biometric Information Protection Act both provide for PRAs, but they are limited to health data and biometric data, respectively. Vermont's legislature passed a bill containing a PRA, but Gov. Phil Scott, R-Vt., vetoed it partly due to the controversial inclusion of a PRA, "which would make Vermont a national outlier, and more hostile than any other state to many businesses and non-profits." This remains the only comprehensive state privacy bill to be vetoed.

So, how does the CCPA's PRA work? Which consumers can sue which businesses over what kind of data breaches, and when?

Jurisdiction

The proceeding analysis is based on cases filed in federal and state courts throughout the U.S., which means they are not all equally weighted. For example, a federal court's interpretation of the CCPA binds other federal courts and non-California state courts but not California state courts because it is a state law. Potential parties should pay careful attention to which authority is binding and which is merely persuasive in the court where they want to file suit.

Trial procedures

None of these cases have made it to a final judgment, which is when the parties go through trial and the judge issues a ruling on which party wins. Instead, they are settled or dismissed, meaning there is more information on the granting or denial of a motion to dismiss than on winning or losing a final judgment.

Requirements to file action under CCPA's PRA

To survive a motion to dismiss, the action must comply with the CCPA's many requirements. First, private plaintiffs may only file actions under the PRA and cannot allege violations of other sections of the CCPA. Second, to fall into the purview of the CCPA's PRA, each plaintiff must be a natural person who is a California resident.

Moreover, each defendant must be a business that collects consumer personal information, determines how and why that information is processed and meets threshold requirements. If the defendant only receives information from a business and processes it according to that business's instructions, then the defendant might be a service provider. Entities can be service providers and businesses at the same time, but people may only bring actions against businesses, not those that are service providers alone.

Third, the action must concern the plaintiff's unencrypted and unredacted personal information. Personal information has a different definition under the PRA than under the rest of the CCPA. For the purposes of the PRA, personal information only contains two categories of information. Under the PRA, personal information can be the plaintiff's first name or initial and last name in conjunction with "data elements" like financial information or personal identifiers. Only one of these, the name or the data elements, needs to be unencrypted or unredacted. Alternatively, personal information can be a way to access the plaintiff's online account, such as username and password or an answer to a security question.

The PRA only concerns allegations that the plaintiff's personal information was "subject to unauthorized access and exfiltration, theft, or disclosure." Some courts have dismissed plaintiffs' CCPA claims because they did not plead specific facts or provide evidence that such a security breach occurred, while others have allowed claims based on allegations that a third party accessed personal information without requiring supporting evidence. One court allowed an allegation of mere potential access and disclosure past a motion to dismiss, so this area is still somewhat murky.

The PRA also requires plaintiffs to allege their personal information was subject to a security breach because the defendant failed to "implement and maintain security practices and procedures," a term not defined in the statute. However, the California attorney general's office has put out nonbinding guidelines for businesses around these practices and procedures, which include recommendations like strong encryption and multifactor authentication.

Medical or health information, which has a specific definition in the statute, is specifically exempted from the PRA. Some plaintiffs filed actions that involve unauthorized access of both their medical and nonmedical information but only claimed violations regarding their nonmedical information. Courts do not agree on whether the CCPA applies to the nonmedical information, but the most recent authority puts the onus on the plaintiff to allege the business treated medical information differently than nonmedical information. One case held that, if a business treats both types as medical information, then it is exempt from the CCPA.

The plaintiff can recover different types of compensation: statutory damages, which are an automatic amount from USD100-750 per consumer per incident, or actual damages, which reflect the amount of money the plaintiff lost due to the breach. Actual damages can include, for example, the cost of identity theft protection or credit monitoring insurance. Plaintiffs can also ask for an injunction or other equitable relief.

If the plaintiff wants to recover statutory damages, they must give 30-day notice to the business of the alleged CCPA violation. Courts disagree on the timing of this notice. Some courts have required plaintiffs to send the notice before filing lawsuits at all. In some instances when the plaintiff did not provide this notice beforehand, the courts dismissed it with prejudice, meaning the plaintiff cannot allege the same claim again. However, other courts dismissed claims without prejudice and allowed plaintiffs to send notice after filing the lawsuits, wait for the required 30 days and then amend their suits to put the claim back in when the business did not cure.

The plaintiff does not need to give this notice or wait for a cure period if they only want to recover actual damages rather than statutory damages.

During the 30-day notice period, if the business "actually cures" the alleged violation and lets the plaintiff know in writing that they cured it, the plaintiff cannot move forward with the claim for statutory damages. As of 1 Jan. 2023, an amendment to the CCPA went into effect that states implementing and maintaining reasonable security procedures and practices in the cure period is not enough to be an actual cure. However, this implementation and maintenance can be an actual cure for incidents involving information collected before 1 Jan. 2023.

Regarding what defendants can do to cure alleged violations, one court held that enhancing security measures is not enough for information collected after 1 Jan. 2023. In two cases, the defendants said they cured the violations, but the courts rejected the arguments because the defendants did not present evidence to back up those assertions.

What claims can plaintiffs allege?

The CCPA plainly states private plaintiffs may not file claims "based on violations of any other section of this title," only the PRA section.

In 2020, after news reports alleged the video communication platform Zoom improperly shared consumer PI, multiple California plaintiffs filed actions under other sections of the CCPA. These included, for example, allegations that Zoom had not provided consumers adequate notice before collecting or disclosing consumer information. Other plaintiffs alleged Zoom did not provide an opportunity for consumers to opt out of selling or sharing their information. The attorney general of California and the California Privacy Protection Agency are the only entities that may enforce other parts of the CCPA, so these claims were facially invalid and immediately dismissed.

What is personal information?

Most of the plaintiffs who brought CCPA PRA actions met the bar for what counts as personal information. However, a complaint regarding general financial information and credit card fraud that did not specifically "allege the disclosure of a credit or debit card or account number, and the required security or access code to access the account" was dismissed because it did "not sufficiently allege disclosure of Plaintiff's personal information."

Security breaches and deficient security management

Plaintiffs may only file lawsuits if their personal information is subject to unauthorized access and exfiltration, theft or disclosure by a third party. This security breach must also be due to a business's failure to implement and maintain reasonable security procedures and practices.

For the first requirement, plaintiffs must allege both components. In Rodriguez v. River City Bank, the court threw out a plaintiff's CCPA claim because he alleged exfiltration, theft or disclosure without alleging unauthorized access.

When plaintiffs do allege both components, courts have differed on what allegations are necessary to sufficiently plead a security breach. Some courts have held that allegations of potential access are enough, while others have held that plaintiffs need to allege that a third party accessed their information. Still others have held that plaintiffs need to provide evidence that a third party accessed their information.

Holdings on this subject have gone back and forth over time. Soon after the PRA came into effect, the court in Stasi v. Inmediata Health Grp., did not dismiss a CCPA claim because "plaintiffs repeatedly allege(d) their information 'was viewed by unauthorized persons'" instead of alleging potential or inferred access.

The court in Mehta v. Robinhood Financial agreed, holding that "alleging that thousands of customer accounts (were) accessed by unauthorized users in a matter of days" was sufficient to allege a security breach. Similarly, the court in M.G. v. Therapymatch did not dismiss the plaintiff's CCPA claim even though he did not allege a data breach, holding that allegations "that defendants disclosed plaintiff's personal information without his consent due to the business's failure to maintain reasonable security practices" was enough to survive. None of these cases required the plaintiffs to allege more specific facts or to provide concrete evidence of these claims at the pretrial stage.

In Kirsten v. California Pizza Kitchen, mere potential access was enough. The court refused to dismiss a claim specifically because "unauthorized parties can access Plaintiffs' (personally identifiable information) on the internet," without mentioning any allegations that this had or had not occurred. However, the court in Lyman v. Kaufman Dolowich Voluck granted summary judgment against the plaintiff partially because he presented "no evidence" that his personal information on Hightail.com, the defendant's website, "was ever accessed by a third party."

Many courts do not mention the security breach prong, or they gloss over it, instead focusing on the second part of this requirement: that the security breach is due to a business's failure to implement and maintain reasonable security procedures and practices.

There is a general trend so far of requiring plaintiffs to allege specific facts regarding what the defendants' security practices and procedures were and how exactly they were deficient. For example, in Maag v. U.S. Bank, Griffey v. Magellan Health, In re Waste Management Data Breach Litigation and Cruz v. Bank of America, the courts all rejected the plaintiffs' CCPA claims because they failed to make such factual allegations about the defendants' security practices and procedures.

Accordingly, courts tend to hold the plaintiff has satisfied the requirements for deficient security management when plaintiffs allege specific facts. In Durgan v. U-Haul International, which survived a motion to dismiss, the defendant did not have adequate email filtering software, train employees, implement multifactor authentication, encrypt personal information or delete it when it was no longer needed.

In In re Sequoia Benefits, the court agreed with the plaintiff's argument that the defendant failed to follow the U.S. Federal Trade Commission's cybersecurity guidelines or other industry standards. The plaintiffs in In re Eureka Casino Breach Litigation also convinced the court by citing FTC guidelines and alleging the defendant failed to monitor for suspicious activity or ensure its vendors had adequate security, among other things.

However, other courts have taken a more lenient stance toward alleging deficient security management, especially early on in litigation. The court in Eureka Casino above also rejected an argument that the plaintiffs did not "provide enough detail about the defendant's former security systems" because the case was still in the early stages of litigation before discovery. In Doe v. MKS Instruments the court similarly held that "in this early phase, Plaintiff's allegations regarding inadequate security procedures are sufficient to state a CCPA claim."

Exceptions and exemptions

The plaintiff in a CCPA PRA action must be a natural person and not a business, per Kostiv and Associates v. Payink, and the defendant must be a business and not a natural person, per Rosado v. Zuckerberg.

A business is an entity that collects consumer data and determines how and why it is processed. If the defendant processes information on behalf of another party and does not make decisions about how it is processed, then the defendant is not a business but a service provider, which is exempt from liability under the PRA per In re In re NCB Management Servers.

The plaintiff in In re Blackbaud adequately alleged the defendant was a business because, among other things, it offered "professional and managed services ... for each of its software solutions" and was registered as a data broker in California, the definition of which requires that the entity be a business. The court in Miller v. Nextgen Healthcare held that using "consumers' personal data ... to develop, improve, and test Nextgen's services' ... is sufficient to satisfy the second requirement."

The CCPA contains exemptions for liability for certain types of businesses, but these do not always overlap with the exemptions in the

PRA specifically. For example, the defendant in Florence v. Order Express tried to argue the CCPA did not apply to it because it is subject to the Gramm–Leach–Bliley Act, but the court dismissed this argument because the statute contains a provision that says this exemption does not apply to the PRA.

Plaintiffs have also explored arguments surrounding the exceptions related to medical information and health care providers. In Stasi v. Inmediata Health Group the court refused to dismiss a claim that involved both medical and nonmedical information. It acknowledged the medical information was exempt, but stated, "Inmediata (did) not address the non-medical information that it admits was accessible on the internet," which allowed the plaintiff's claim to survive. The court did not mention the entity-level exemption.

However, the court in Tate v. EyeMed Vision Care declined to follow Stasi's lead and dismissed the claim because the plaintiff failed "to provide specific allegations that EyeMed (maintained) non-medical patient information in a different manner than medical information — a fact required to establish the California statute covers EyeMed." The court in Lurry v. PharMerica agreed with Tate and dismissed a claim for the same failure to allege different treatment of medical and nonmedical information.

Because the Stasi court did not mention the entity-level exemption, this portion is dictum and does not bind future courts' decisions, but the structure of the analysis suggests defendant Inmediata had the responsibility to claim it maintained medical information differently than nonmedical information. The courts in Tate and Lurry instead dismissed their respective CCPA claims because the plaintiff failed to make the same allegation, effectively flipping the requirement to the other party.

Notice, cure period and timing

The court in Gardiner v. Walmart held the CCPA only applies to violations of the duty to implement and maintain reasonable security procedures and practices that occurred on or after 1 Jan. 2020.

To recover statutory damages, the plaintiff must give a 30-day notice and may only proceed with filing the claim for statutory damages if the defendant does not actually cure the alleged violation. For example, the court in Lyman v. Kaufman Dolowich Voluck granted summary judgment for the defendant because the plaintiff provided no evidence that he had ever given notice.

The court in Griffey v. Magellan Health Inst. dismissed a CCPA claim with prejudice because the plaintiff filed a complaint demanding both actual pecuniary and statutory damages without giving notice beforehand, holding that "if a notice filed before the 30-day deadline could be updated when an amended complaint is filed and satisfy the 30-day notice requirement, then having the pre-suit notice requirement would be pointless." Two other courts in Golden v. Onetouchpoint and Guy v. Convergent Outsourcing also dismissed the claims, but gave the plaintiffs leave to amend and put the claims back in after the notice-and-cure period passed.

A later court in In re LastPass Data Security Breach Litigation analogized the notice requirement to a similar requirement in the

California Consumer Legal Remedies Act, under which "some courts have held that notice sent thirty days prior to the operative complaint suffices," meaning the claim would not be barred as long as the plaintiffs have filed an amended complaint more than 30 days after sending notice. The court in In re Eureka Casino Breach Litigation agreed and allowed a claim where the plaintiff provided CCPA notice and filed an action on the same day, then amended the complaint to include a CCPA claim four months later.

Another court in In re San Francisco 49ers Data Breach Litigation declined to hold one way or another because the issue remained "in question," instead directing the parties to come to an agreement among themselves as to whether the plaintiffs could argue the claim.

Even when a plaintiff provides notice, it is not yet clear what actions can sufficiently cure an alleged breach. As of 1 Jan. 2023, an amendment to the CCPA took effect, stating "the implementation and maintenance of reasonable security procedures and practices does not constitute a cure with respect to (a) breach" for which the business has received notice.

Few cases address this newer standard, but those that do have cut toward the plaintiffs. In Florence v. Order Express, the court refused to dismiss the plaintiff's claim based on the defendant's "bare assertion in the motion to dismiss that it 'cured all alleged violations within the requisite time period.'" The defendant in Prutsman v. Nonstop Administration also said in its letter to the plaintiff that it had cured the CCPA violation, but the court also refused to dismiss the claim because this statement did "not render implausible plaintiff's allegations to the contrary." The court in Sequoia Benefits agreed with this reasoning.

Settlements

So far, every case that has survived a motion to dismiss has been settled. Cash penalties vary from case to case depending on how severe the alleged violation was, how many people were affected and other factors, but other common themes have emerged. For example, some settlements have required defendants to implement improved security measures or pay for identity protection and credit monitoring after a data breach.

The first class-action settlement under the CCPA PRA, In re Hanna Andersson, saw the defendant company create a settlement fund of USD400,000. Class members were entitled to up to USD500 for a basic award and up to USD5,000 to reimburse losses like unauthorized charges and out-of-pocket expenses. The defendant also committed to "take reasonable steps to secure access to (its) e-commerce platforms," which included conducting risk assessments, enabling multifactor authentication and hiring additional technical staff.

The settlement in In re California Pizza Kitchen Data Breach Litigation saw similar terms: California class members could recover USD100 as statutory damages, members who incurred out-of-pocket expenses could recover up to USD1,000 and members who had monetary losses as a result of actual identity theft could recover up to USD5,000. California Pizza Kitchen also provided two years of credit monitoring and agreed to take remedial measures, again including implementing multifactor authentication. This settlement stands out from the rest because it had no dedicated settlement fund; the only limit on the fees California Pizza Kitchen would pay depended on how many class members claimed their benefits.

To date, the largest publicized settlement was in In re T-Mobile Data Security Breach Litigation. T-Mobile created a USD350 million settlement fund from which California class members could recover USD100 in statutory damages and all members could recover up to USD25,000 for out-of-pocket losses and up to USD375 for lost time. All members were entitled to two years of identity theft protection and insurance, credit monitoring and restoration services, which included "access to US-based fraud resolution specialists who can assist with important tasks" related to identity theft and members' credit. The agreement also included a requirement for T-Mobile to spend at least USD150 million above its previous budget for 2022-23 on "data security and related technology."

Conclusion

Plaintiffs, defendants and courts alike are still feeling out the edges of what the PRA does and does not allow. Five years of litigation and hundreds of cases filed across the U.S. still make this area of jurisprudence relatively underdeveloped compared to most other areas of the law.

Many factors contribute to the lack of consensus in CCPA PRA cases. Both sides feel the pressure to settle disputes quickly so defendants do not have to admit fault, plaintiffs can recover money quickly without waiting months or years for a verdict and both sides can avoid creating potentially disadvantageous precedent in the future. Even the text of the CCPA remains in flux as it receives amendments to keep it relevant to the blistering pace of technological development.

Even if litigation under the CCPA's PRA is unlikely to reach equilibrium for years, if not decades, parties and their lawyers in these early stages have built litigation strategies based on preliminary impressions. Developments may be slow to manifest, but understanding will grow over time as more arguments and opinions shape what the PRA comes to mean for individuals and businesses.