Alliant

California Privacy Rights Act: A Harbinger of Things to Come?

By, David Finz, Vice President, Cyber Claims, and Robert Horn, Co-Cyber Product Leader

California has been at the forefront of privacy regulation from the outset. They were one of the first states to require that notification of a breach be given to impacted parties. On January 1, 2020, the California Consumer Privacy Act (CCPA) became effective. The CCPA created a private right of action under statute for individuals whose information had been breached and also set forth data management requirements for companies doing business with California residents.

However, one key limitation of the CCPA was its provision that only the California Attorney General had the authority to bring an enforcement action for violations of the law which did not involve a data breach. The Attorney General's office has made clear from the law's enactment that it lacks the resources to prosecute such cases under the CCPA. Some privacy experts also expressed concern that the CCPA did not clearly delineate the obligations of vendors who may receive personal information through the company to whom they are providing services, rather than directly from the consumer.

Consumer Privacy with Teeth

As a result of this lack of enforcement activity and unclear wording, privacy rights activists launched a campaign to pass additional legislation. In November of 2020, voters approved a referendum (known as Proposition 24) which resulted in the enactment of the California Privacy Rights Act (CPRA). The CPRA created a new enforcement body called the California Consumer Protection Agency, and vested within it the same authority as the state Attorney General previously had. The new agency can commence actions against companies to enforce the law, even if there was no breach of personal information. Additionally, in an effort to reduce the prevalence of "targeted ads," the CPRA enables consumers to opt-out of permitting websites they visit to share their data.

The CPRA has also clarified what the obligations are for a company's service providers. Under this new statute, any third party (such as a payment processor or cloud provider) that is entrusted with a consumer's data is under the same compliance obligations, not only with the law, but with whatever additional protections a business may have offered (and which the consumer may have relied upon) in the original business transaction.

Other States Follow Suit

The history of data privacy shows that laws enacted in California are often replicated elsewhere. For example, in the past year alone, Colorado and Virginia have enacted comparable laws, and several other states are considering similar legislation. Some observers have noted that California seems to be taking its cue from the European Union's General Data Protection Regulation (GDPR), which relies upon "Information Commissioner's Offices" in its member countries for enforcement.

Preparing Your Organization

One question which remains is how these cases will be tried and settled. Even if a Plaintiff were to survive a Motion to Dismiss, damages may be difficult to quantify. One option may be for the parties to enter into a consent decree, whereby as part of the settlement, the Defendant agrees to take certain actions to bring its business practices into compliance with the CPRA. As part of that consent decree, the Plaintiff may be awarded attorney's fees as the prevailing party in the underlying case. This could have the effect of incentivizing further private party litigation, since the Plaintiffs' bar would be rewarded for its efforts in bringing such actions.

For companies doing business in California, they should already be complying with the CCPA, which encompasses many of the CPRA's requirements. Now, though, downstream business partners are also bound by whatever privacy practices their client had in place for its own customers. For example, a direct mail company that receives leads from a magazine would need to comply not only with the CPRA, but with whatever privacy protections the magazine offered to its subscribers when they chose to entrust the magazine publisher with their personal data. This is a statutory duty on the part of the vendor which cannot be contracted away by the parties when drafting a service agreement, since it is designed to protect consumers.

Put another way, when it comes to consumer protections, the CPRA is a floor, not a ceiling. Because of this, it's critical for service providers to understand how their client's privacy policy applies to any data the service provider will be handling. Additionally, as other states begin to adopt similar laws, companies will want to standardize their data management practices to the extent possible in order to stay in compliance with the most stringent requirements in the patchwork of legislation we can expect to develop over the next several years.

Is It Covered? Insurance Implications

Most Cyber policies already define privacy regulation broadly enough to pick up actions brought under any state, federal or foreign law, such as the GDPR. However, it's important to make sure that the coverage for regulatory proceedings isn't solely triggered by a breach event. Otherwise, a wide range of violations (such as wrongful collection, failure to encrypt after promising to do so, unclear opt-out provisions, or failure to dispose of data at the consumer's request) would not trigger coverage under the Insured's Cyber policy. Simply put, there doesn't necessarily have to be a data breach for there to be a violation of data privacy legislation, and the coverage should respond accordingly. Businesses have been facing this reality in other jurisdictions as well, such as in Illinois, where the Biometric Information Privacy Act (BIPA) permits private rights of action even when no breach has occurred.

Another question which arises is whether fines and penalties imposed under data privacy statutes are insurable by law. Since these losses are not insurable in some jurisdictions, the preferred policy wording covers regulatory fines and penalties, "where insurable by law." Additionally, because a coverage dispute may be subject to the law of multiple jurisdictions (e.g., the state where the underlying claim arose, the state where the policy was delivered to the Insured, the domicile of the Insurer), the policy should further provide that for purposes of determining the insurability of fines and penalties, the law of the jurisdiction most favorable to the Insured shall govern.

Conclusion

As regulations continue to proliferate and Plaintiffs devise new theories of liability and damages, it's essential for businesses to have a comprehensive strategy around data privacy and risk transfer. This is where a qualified insurance advisor can help guide companies in their decisions.

Cyber Risk and Network Security

Your company takes advantage of the latest advances in technology, but is it ready to respond to the most recent cyber risks? Today's companies can fall victim to a multitude of cybercrimes. The damage caused by any of these losses could be substantial. Costs can escalate rapidly, and with computer-related events increasingly excluded from general liability policies, it's easy to see why cyber liability insurance is necessary.

All privacy and cyber liability insurance policies are different, and coverage terms can change as quickly and as rapidly as the risks they cover. That's why it takes a specialist that can help you tackle the moving risks posed by technology, assess those exposures that threaten your company or organization, and identify the coverage that matches your risk profile.

As the nation's premier specialty retail insurance brokerage company, Alliant Insurance Services has been ahead of the game at every turn in the market. Our reputation has been built on the depth of experience and breadth of resources that are devoted to developing thoughtful solutions that guard our clients against emerging risks.

For more information:

David Finz
Vice President, Cyber Claims
David.Finz@alliant.com
631-356-2483

Robert Horn
Co-Cyber Product Leader, Cyber Claims
Robert.Horn@alliant.com
212-504-5828