JENNER & BLOCK

"Beware of Loopholes in Privacy Insurance Policies for California," *Bloomberg Law*

Publications

September 4, 2025

The California Invasion of Privacy Act creates a private right of action for individuals who have been the victim of, for example, the wiretapping of their telephone lines. With dramatic advances in technology, private plaintiffs have filed CIPA claims connected to customer service call recordings, transcription services, and website chat services.

Plaintiffs in *Rodriguez v. Ford Motor Co.* and *James v. Allstate Ins. Co.* argued that the defendants violated their CIPA rights—or aided and abetted such violations—by disclosing communications to a third party or permitting that third party to monitor the communications.

While both cases were dismissed, defending these types of actions is costly. Thus, companies facing CIPA actions may want to consider turning to their insurance policies as a potential source of coverage.

Cyber liability insurance, for example, typically provides coverage for a cyber incident or data breach, but it also may cover the alleged improper or unauthorized collection, retention, or disclosure of private information by an insured.

Insurance policies for commercial general liability, or CGL, cover broad alleged bodily injury, property damage, and other types of personal and advertising injuries (which often include alleged privacy violations).

Reviewing Exclusions

Once an insured can show that a CIPA claim falls within its policy's grant of coverage, it must review the policy's exclusions and other limitations to determine whether any preclude coverage.

Several types of common exclusions should be avoided, if possible, as part of the initial policy negotiation and placement process.
Cyber liability policies may exclude alleged violations of certain privacy statutes, including the Illinois Biometric Information Privacy Act, or BIPA. Others are more broadly worded to include similar federal, state, or local statutes and can sweep in additional underlying actions as new

statutes continue to be enacted nationwide. Cyber liability policies also may exclude alleged eavesdropping or improper or unauthorized collection and tracking of personal information.

CGL policies may exclude claims arising from an insured's alleged statutory violation. While these exclusions may specify certain statutes, they also may contain more general, catchall language designed to exclude any defense fees or damages from claims alleging a state or federal statute violation. CGL policies also may contain access and disclosure language that purport to exclude claims that an insure allegedly retained improper or unauthorized access and disclosure of personal information.

Insurance policies typically bar coverage for claims arising from the insured's alleged intentional conduct. As such, an insurer could argue that if an insured deliberately tracked and collected personal data, any alleged CIPA violation was intentional and must be excluded from coverage.

Insureds must focus their attention on arguments as to why such exclusions shouldn't apply based on the specific language in their policies and the particular allegations in the underlying action.

BIPA Challenges

While courts appear not to have directly examined the extent to which cyber liability and CGL insurance policies may respond to CIPA claims, the way in which courts have addressed insurance coverage for alleged BIPA violations is instructive.

BIPA is a statute intended to protect individuals against unauthorized collection, retention, and disclosure of their biometric information, such as fingerprints. Defendants facing BIPA allegations historically have turned to cyber liability and CGL policies as a potential source of insurance coverage. In response, insurers have raised exclusions concerning access and disclosure and statutory violations.

Following years of litigation examining these two exclusions, the US Court of Appeals for the Seventh Circuit in May assessed the applicability of each exclusion in *Citizens Insurance Company of America v. Mullins Food Products, Inc.* The defendant-insured has turned to its CGL insurance policy to fend off a BIPA claim that it collected and disclosed employees' biometric information to a third part for employment-related purposes. But the insurer sought a declaration federal court that no coverage existed, citing the access and disclosure and statutory violation exclusions in the policy. The district court granted summary judgment in favor of the insurer, finding the exclusion language barred coverage.

The Seventh Circuit agreed that the access and disclosure exclusion unambiguously applied to bar coverage. Because personal information "plainly includes biometric identifiers," there was "no reasonable doubt that the exclusion excludes coverage for BIPA claims."

The court reached the opposite conclusion concerning the statutory violation exclusion, which barred coverage for "personal and advertising injury arising directly or indirectly out of any action or

omission that violates or is alleged to violate" the Telephone Consumer Protection Act, the CAN-SPAM Act of 2003, and Fair Credit Reporting Act.

The exclusion contained catchall language barring claims arising out of violations of and "federal, state or local statute, ordinance or regulation, other than the TCPA, CAN-SPAM Act of 2003 or FCRA and their amendments and additions, that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information."

The court concluded that the catchall provision didn't apply, reasoning that the nature of the statutes cited concerned communications and credit reporting history, which are "patently different in kind" from the information protected by BIPA. Turning back to alleged CIPA violations, the reasoning in *Citizens* suggests these exclusions continue to be relevant in assessing whether insurance coverage is available for an underlying action involving CIPA claims. Unlike biometric identifiers, it's unclear that customer service calls and website chats are plainly included as personal information, and whether they qualify as personal information may depend on the facts of the case.

Insurers may argue that CIPA does indeed regulate communications, at least in the form of eavesdropping, and the type of catchall language at issue in the statutory violation exclusion in *Citizens* could apply.

While specific policy language and allegations at issue in the underlying action ultimately will determine the availability of insurance, insureds facing CIPA actions should be aware of the kinds of insurance policies available and the types of exclusions and limitations that insurers are likely to raise.

***

Related Attorneys

Jan Larson
Partner
janlarson@jenner.com
+1 213 239 2273

Steven Tinetti
Associate
stinetti@jenner.com
+1 312 840 7360

Related Capabilities

Insurance Recovery and Counseling

Related Locations

Los Angeles

Chicago

Stay Informed →