Client Update
No Coverage Under Commercial General Liability Policies in Recent Data Privacy Suits

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Andrew M. Levine
amlevine@debevoise.com

Keith J. Slattery
kjslattery@debevoise.com

WASHINGTON, D.C.
Sisi Wu
swu@debevoise.com

Two federal courts recently held that, under commercial general liability ("CGL") policies, insurance companies did not owe policyholders a duty to defend against consumer suits alleging electronic violations of privacy. Although specific to the facts and policies at issue, the decisions highlight the uncertainty in relying on traditional CGL policies for data privacy and breach coverage. The decisions also highlight the need for companies, their risk managers, insurance brokers and counsel to consider: Should a company have coverage specific to the privacy and cyber space, or is CGL coverage sufficient notwithstanding court decisions like these? If privacy- and cyber-specific coverage is desirable, what kind, and in what amounts?

WHAT HAPPENED?

Defender Security Company, a home security systems provider, allegedly recorded and stored all incoming and outbound phone conversations without notice or consent. Defender was hit with a state court class action in California, asserting violations of the California Penal Code. Sections 632 and 632.7 of the Code make it unlawful to record telephone and cellular communications without consent.

Aspen Way Enterprises, a franchisee of the Aaron's rent-to-own business, allegedly installed spy software on laptops that it leased to customers. The software allegedly allowed Aspen Way to access personal data such as images taken from webcams, keystrokes and screenshots. A federal class action filed on behalf of Aspen Way customers asserted claims under the Electronic Communications Privacy Act, 18 U.S.C. § 2511, and a common-law invasion of privacy claim. The State of Washington also sued Aspen Way, asserting violations of state consumer protection and spyware laws.

THE COURT RULINGS: CGL COVERAGE DOES NOT APPLY

Defender and Aspen Way each sought coverage for these suits from various insurers under CGL policies. The insurers denied coverage.

Defender sought a declaratory judgment that its insurer owed it a duty to defend. Defender's insurer prevailed on a motion to dismiss in the trial court; that dismissal has just been affirmed by the U.S. Court of Appeals for the Seventh Circuit.

Aspen Way's insurers sued in separate actions seeking declaratory judgments that they did not owe a duty to defend the company. The U.S. District Court for the District of Montana ruled in favor of the insurance companies.

Both Defender and Aspen Way relied on policy provisions that provided for defense against suits alleging "personal or advertising injuries." Critically, the policies defined such injuries in part as those arising out of "oral or written ***publication*** of material that violates a person's right of privacy." (emphasis added)

With respect to Defender, the Seventh Circuit held that the mere recording and storage of information could not reasonably be construed as "publication." The carriers therefore did not owe a duty to defend.

With respect to Aspen Way, the district court determined that the Washington State suit did not allege facts amounting to publication of information, but that some claims in the underlying consumer class action did sufficiently allege publication and therefore triggered possible coverage. This included transmission of captured customer data to the software developer and to Aspen Way. Even with such publication, however, the court ruled that Aspen Way's insurers did not owe a duty to defend given exclusions in the policies denying coverage for actions that may have violated statutes governing the recording and distribution of information. The district court concluded that the exclusions applied here because Aspen Way may have violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511, when customers' personal information was captured and transmitted without their knowledge. The court also concluded that one of the insurance policies was not triggered because it expired prior to the alleged misconduct.

These decisions resonate with last year's decision by a New York trial court in the coverage dispute between Sony and its insurer regarding data breach claims arising from the 2011 cyberattack on Playstation. There too, the court concluded

that the "publication" provision of a CGL policy could not be extended to cover cyber claims. The dispute was resolved by the parties before disposition of Sony's appeal.

WHAT NEXT?

In each of the Defender, Aspen Way and Sony matters, the courts declined to construe older CGL policies to cover privacy and cyber risks, at least where "publication" was the asserted basis for coverage. Although the outcomes of such cases necessarily hinge on the particular facts and policies at issue, the decisions underscore that relying on traditional CGL policies to cover privacy and cyber risks remains far from certain. Meanwhile, new CGL policies may expressly exclude privacy and cyber risks. Companies thus should assess their privacy and cyber exposure, and consider the desirability of policies that expressly cover these risks.

Because actuarial data relating to data privacy issues and security breaches remains limited, it is difficult for underwriters to quantify risks. Insurers writing this coverage will rely on qualitative assessments of applicants' risk profiles. They also will look at how well a company can document its risk management procedures and risk culture. Companies considering or seeking such coverage will do best in the underwriting process if they understand and can articulate their risk management posture. A company's ticklist might include:

- Understanding the types of data collected and stored by the company;
- Assessing the volume and location of records that contain personally identifiable information or other sensitive confidential information;
- Preparing, testing and regularly updating an incident response plan for handling any actual breach, whether caused by an external hacker or internal missteps;
- Carefully measuring and documenting the company's privacy and cybersecurity posture in light of recognized benchmarks such as the Framework issued by the National Institute of Standards and Technology;
- Building the internal team and the roster of outside advisors (e.g., cyberforensics consultants, crisis management firms and, yes, lawyers) necessary to assess and constantly improve the company's cybersecurity posture; and
- Ensuring that any outside vendors who have access to the company's network, or to whom the company outsources sensitive data, are

contractually bound to – and do – also follow robust security and privacy practices.

The decisions are *Defender Security Company v. First Mercury Insurance Company*, No. 1:13-cv-00245 (7th Cir. Sept. 29, 2015) and *American Economy Insurance Company v. Aspen Way Enterprises*, No. 14-cv-09 (D. Mont. Sept. 25, 2015). Our Cybersecurity/Data Privacy and Insurance teams are available to discuss.

Please do not hesitate to contact us with any questions.