Broad Implications

Coverage Issues Arising from Cyber Security Breaches

By Laura A. Foggan and Edward R. Brown

Courts have signaled strongly that policyholders cannot rely on commercial general liability coverage to address the exposures posed by data breach and cyber claims.

Recall Total Information Management, Inc., et al., v. Federal Insurance Co., et al., No. SC 19291, 115 A.3d 458, (Conn. May 18, 2015), is a critical ruling with wide-reaching implications. Many in the coverage world—both on the insurer and on the policyholder side of the aisle—viewed *Recall Total* as a test case for the limits of commercial general liability (CGL) policies in the data breach context. *Recall Total* lived up to its billing, and it serves as an important rejection of the notion that data breaches are covered by CGL policies. Crucially, the policies in *Recall Total* did *not* contain specific exclusions for breaches of privacy liability, which have widely been used to confirm the coverage intent in later forms, but the court still rejected policyholder arguments that the absence of such exclusions somehow dem-

■ Laura A. Foggan is a partner, and Edward R. (Ted) Brown is an associate, of Wiley Rein LLP in Washington, D.C. Ms. Foggan, who chairs the firm's Insurance Appellate Practice, regularly handles emerging risks, data breach and cyber liability coverage, environmental coverage, product liability, construction, personal and advertising injury, and bad faith. Mr. Brown represents insurers in coverage litigation before federal and state courts. He serves as coverage counsel for claims under general liability and various types of professional liability policies, and he regularly counsels insurers in connection with claims involving data security and privacy breaches.

onstrated that coverage was available for data breach exposures. The court enforced the unambiguous limitations of "Coverage B," the personal injury coverage part, of the CGL policies in finding no coverage.

After the Connecticut Supreme Court issued its decision in *Recall Total*, many policyholder advocates tried to cast the *Recall Total* decision as an outlier, limiting it to its specific facts. However, the policyholders and their amici in the *Recall Total* case recognized its broad significance.

For example, United Policyholders, a California-based organization that advocates for large corporate as well as individual consumer policyholders, appeared as amicus curiae in *Recall Total*. United Policyholders contended that *Recall Total* was a key test of the extent to which data breach overage is available under general liability policies. Indeed, its amicus brief emphasized that "[t]he question presented in this case is of importance to insurance consumers across the nation, particularly consumers of commercial general liability ("CGL") policies, because data security is continuing to rise as an issue that corporations confront in day-to-day operations." Br. of Amicus Curiae United Policyholders in Support of Plaintiffs-Appellants' Br. on the Merits, at 1.

Further, the United Policyholders brief also made clear that in *Recall Total* the breach presented very much the same way as a "typical" data breach, comparing "[t]he loss of the unencrypted data on the tapes [in *Recall Total*]," for instance, to a breach that had involved employee data "contained in a computer file that was unintentionally attached to an email and sent to a third party." *Id*. at 4. The United Policyholders brief also stated:

> Corporations are required under state laws to take immediate mitigating measures when a data breach occurs, which can cost hundreds of thousands of dollars or more. These corporations, as consumers of commercial general liability policies, reasonably rely upon their commercial general liability insurance—and the personal and advertising injury coverage in particular—to protect them in the event of such a loss.

Id. at 1–2.

Of course, the *Recall Total* ruling squarely rejected CGL coverage for such "mitigating measures" because the more than $6 million in "mitigating" expenses that IBM incurred were not covered losses "since merely triggering a notification statute is not a substitute for a personal injury." *Recall Total Information Management, Inc. v. Federal Ins. Co.*, 83 A.3d 664, 673 (Conn. App. Ct. 2014); *Recall Total,* 115 A.3d at 460 (adopting without repeating the opinion in *Total Recall*, 83 A.3d 664 (Conn. App. Ct. 2014)).

As these arguments demonstrate, policyholder advocates understood the broad implications that the *Recall Total* decision would have for data breach cases. The Connecticut high court's ruling makes clear that CGL policies are not a solution for managing data breach and cyber breach events. This conclusion, moreover, is reinforced by other early precedents addressing whether CGL policies cover cyber liabilities.

Recall Total Ruling

In *Recall Total*, a records storage company and its transportation subcontractor, both of which were insureds under certain insurance policies, had agreed to transport and store various electronic media belonging to IBM, a client of the storage company. During transport, a cart containing employment-related data tapes for past and present IBM employees fell out of the back of the transport van and onto the roadway. Some of the tapes were never recovered and were believed to have been stolen by an unknown third party. IBM spent approximately $6 million taking remedial actions, including providing security breach notifications and identity theft protection for employees whose information was on the tapes. IBM sought to recover those expenses from the records storage company and transportation subcontractor. IBM and the storage and transport companies engaged in nearly two years of settlement negotiations before ultimately reaching a settlement.

> ***Recall Total* lived up** to its billing, and it serves as an important rejection of the notion that data breaches are covered by CGL policies.

The records storage company and the transportation subcontractor sought coverage from their CGL insurers for the costs of the negotiations and the amounts at issue. After the insurers denied coverage, the records storage company and transportation subcontractor sued for breach of contract. The Connecticut trial court ruled that the insurers had not breached their duty to defend and that the insureds' loss was not covered under either Coverage A (property damage liability), or Coverage B (the personal injury provision), of the relevant CGL policies.

On appeal, the Connecticut intermediate appellate court rejected the effort to recover costs of the settlement negotiations, ruling that the settlement negotiations did not constitute a "suit" or "other dispute resolution proceeding" under the terms of the policies. The court considered whether settlement negotiations in response to a demand consti-

tuted a "suit," which was defined in relevant part in the policy as "a civil proceeding in which damages, to which this insurance applies, are sought… [and] includes arbitration or other dispute resolution proceeding… to which the insured must submit or does submit with our consent." Concluding that the settlement negotiations did not constitute a "suit," the court reasoned that to "construe 'suit' to include mere negotiations following a demand would obliterate the distinction between 'suit' and 'claim.'" The court explained that under the policy, the policyholder owes a duty to the insurer to provide notice of both "claims" and "suits," but the insurer only has the duty to defend against "suits." The court also rejected the argument that the settlement negotiations constituted an "other dispute resolution proceeding" because interpreting "suit" that broadly would mean that "every discussion, however informal, between an insured and a third party could be deemed a dispute resolution proceeding." While the Connecticut Supreme Court also adopted this part of the ruling, it is not discussed further here because the focus of this article is the cyber and data breach aspects of the *Recall Total* ruling.

In tort claims arising from data breaches, many courts have found that the absence of concrete injury dooms claimants' data breach suits because the claimants cannot show that they were harmed from the breach.

As for the scope of CGL coverage for data breach, the intermediate appellate court held that the actual loss of the data tapes did not constitute a covered "personal injury," defined in Coverage B of the policy as "injury, other than bodily injury, property damage, or advertising injury, caused by an offense…." The covered offenses included "electronic, oral, written, or other publication of material that… violates a person's right to privacy." In holding that the loss of the data tapes did not fall within the coverage parameters, the court noted the absence of evidence showing that any individual had actually accessed the information on the tapes. Further, the court held that the costs of security breach notifications were not covered damages due to violations of a person's right of privacy. The Connecticut intermediate appellate court determined that "notification statutes simply do not address or otherwise provide for compensation from identity theft or the increased risk thereof, [sic] they merely require notification to an affected person so that he may protect himself from potential harm. Accordingly, merely triggering a notification statute is not a substitute for a personal injury." 83 A.3d at 673.

After the Connecticut intermediate appellate court issued this detailed decision, the records storage company and transportation subcontractor appealed to the Connecticut Supreme Court. The Connecticut Supreme Court squarely rejected coverage and affirmed the intermediate appellate court's decision on all of the coverage issues. In adopting the decision below, the Connecticut high court stated:

> We… granted the plaintiffs' petition for certification to appeal from the judgment of the Appellate Court, limited to the following issue: ''Did the Appellate Court properly affirm the trial court's summary judgment rendered in favor of the defendants?'' *Recall Total Information Management, Inc. v. Federal Ins. Co.*, 311 Conn. 925, 86 A.3d 469 (2014). Our examination of the record and briefs and our consideration of the arguments of the parties persuade us that the judgment of the Appellate Court should be affirmed.

Because it found that the intermediate appellate court's well-reasoned opinion fully addressed the certified issue, the Connecticut Supreme Court "adopted the Appellate Court's opinion as the proper statement of the issue and the applicable law concerning that issue." *Recall Total,* 115 A.3d at 460 (citing *Citizens Against Overhead Power Line Construction v. Connecticut Siting Council*, 86 A.3d 463 (Conn. 2014)).

Through this ruling, the Connecticut Supreme Court has made clear that CGL policies' Coverage B cannot be stretched to provide data breach coverage for security breach notification and losses such as those in *Recall Total*.

Recall Total Rationale

There are a number of different reasons why CGL coverage was not implicated in *Recall Total*, but all paths led to the same place: a determination that there was no coverage. These same limitations apply in a host of other factual scenarios as well. While policyholders will likely continue to test Coverage B, and commentators belatedly have sought to distinguish the facts in this case from other data breach scenarios, the *Recall Total* court's ruling contains reasoning and language that does not limit its application to the specific facts in that case.

In *Recall Total* and other cases that involve lost hardware, lost electronic storage devices, or encrypted data exfiltration, the loss of those storage devices or the loss of the encrypted data would not fall within the coverage parameters because these "offenses" do not amount to injurious "publication" of "material that violates a person's right to privacy." *See State Farm Gen. Ins. Co. v. JT's Frames, Inc.*, 104 Cal. Rptr. 3d 573, 586 (Cal. Ct. App. 2010). Stated differently, as the *Recall Total* court made clear, there is a critical distinction between the disclosure of the information contained in a storage medium or encrypted file and the loss of the medium or file itself. *See, e.g.*, *Whole Enchilada, Inc. v. Travelers Prop. Cas. Co.*, 581 F. Supp. 2d 677, 696–97 (W.D. Pa. 2008) (no "publication" where information was not "made generally known, publicly announced, []or disseminated to the public"); *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 444 Fed. App'x 370, 375–76 (11th Cir. 2011) (the phrase "publication, in any manner" was unambiguous and did not apply when there was no dissemination of information to the general public); *Terra Nova Ins. Co. v. Fray-Witzer*, 869 N.E.2d 565, 572 (Mass. 2007) (the phrase "publication" was unambiguous and meant "'communication (as of news or information) to the public' or a 'public announcement'" and was satisfied by a mass transmission

of 60,000 advertisements). In *Recall Total*, as in many data breach cases, there was no evidence that information was ever accessed by any third party; instead, the data tapes were simply known to have been lost, but whether or not or how data was used after that was nothing more than a matter of conjecture. And as the court noted in *Recall Total*, the triggering of a breach notification statute cannot serve as a "substitute for personal injury."

Also, when the individuals whose information was compromised have not experienced harm, there can be no "personal injury." In tort claims arising from data breaches, many courts have found that the absence of concrete injury dooms claimants' data breach suits because the claimants cannot show that they were harmed from the breach. *See, e.g.*, *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 12-347(JEB), 2014 WL 1858458, at *6–*8 (D.D.C. May 9, 2014) (rejecting standing based on alleged "risk of identity theft" and "cost of credit monitoring and other preventative measures"). Here, the *Recall Total* ruling found that notification costs are not a substitute for the requirement that there was an actual injury to privacy interests, let alone one insured under a CGL policy. In *Recall Total*, the insureds claimed that "[b]ecause state privacy protection laws presume publication and misuse of the stolen data, the circumstances of loss and theft of the… tapes [in *Recall Total*] establish at least an inference that a publication and invasion of privacy has occurred." Br. of the Plaintiff-Appellants, Recall Total Information Management, Inc. and Executive Logistics Services, Inc., at 25. The insureds in *Recall Total* also claimed that the costs of notification and offering credit monitoring were loss "from the violation of privacy rights that the state laws and policy presume has occurred." *Id.* at 27. The Connecticut Supreme Court squarely rejected these arguments, however, rightly concluding that "merely triggering a notification statute is not a substitute for a personal injury."

Significance of *Recall Total* and Other Cases Addressing CG Coverage for Data Breaches

As they did in *Recall Total*, policyholders often argue that statutory notification obligations act to trigger coverage. The court's rejection of this argument in *Recall Total*, however, provides a strong precedent for future cases. Breach notification statutes may be triggered under a wide range of circumstances, including experiencing data-tape or hard copy "paper file" losses or losing a device such as a laptop or cell phone, even without any actual proof that information was accessed or resulted in harm to individuals. The same is true for certain system intrusions. Companies that experience system intrusions may have statutory notification obligations even if there may be no actual proof of access to specified personal information, or companies may have notification obligations if they discover vulnerabilities in a system even if it is unclear whether or the extent to which sensitive data was compromised. However, when private information is not released to the public, and there is not even proof of *any* third-party access to the information, "publication" plainly has not taken place. *Recall Total* stands for the broad proposition that a state notification obligation cannot serve as a substitute for the elements needed to trigger Coverage B. Thus, the Connecticut high court's ruling is not an outlier that is limited to quirky facts, as many advocates now claim it to be. Instead, *Recall Total* is a significant ruling with effects that extend to a wide range of data breach scenarios.

Other early cases addressing policyholder efforts to shoehorn cyber losses into CGL policies reinforce the conclusion that CGL coverage is not a panacea for cyber liabilities. Importantly, Coverage B only affords coverage for enumerated "offenses," which involve specified acts by a policyholder. In fact, many courts have ruled that personal injury provisions reach only purposeful acts by the insured. *See, e.g.*, *Cnty. of Columbia v. Cont'l Ins. Co.*, 634 N.E.2d 946, 950 (N.Y. 1994) ("[C]overage under the personal injury… provision… was intended to reach only purposeful acts undertaken by the insured or its agents."); *Gregory v. Tenn. Gas Pipeline Co.*, 948 F.2d 203, 209 (5th Cir. 1991) (personal injury coverage "requires active, intentional conduct by the insured"); *Harrow Prods. v. Liberty Mut. Ins. Co.*, 64 F.3d 1015, 1025 (6th Cir 1995) (holding that each enumerated offense in Coverage B requires an intentional act); *Butts v. Royal Vendors, Inc.*, 504 S.E.2d 911, 917 (W. Va. 1998) (coverage for "[o]ral or written publication of material that violates a person's right of privacy" not triggered when allegation was that the insured induced a third party to publish material that violated the claimant's rights); *Arrowood Indem. Co. v. Oxford Cleaners & Tailors, LLC*, No. CIV. 1:13-12298-PBS, 2014 WL 4104169, at *8 (D. Mass. Aug. 15, 2014) (holding that "personal and advertising injury" offenses must be interpreted "in light of the words around [them]" and that claims for negligence are not sufficient to trigger these provisions); *Stonelight Tile v Cal. Ins. Guar. Ass'n*, 58 Cal. Rptr. 3d 74, 89 (Cal. Ct. App. 2007) (noting that Coverage B offenses are based on intentional conduct, and not accidental conduct).

Indeed, in another major data breach case addressing CGL personal injury coverage, a court held that there was no coverage because there was no wrongful offense by the policyholder. *See Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014). In *Sony*, the offending act was perpetrated by hackers, not a "publication" undertaken by the insured, and thus the court ruled that there was no coverage. Almost by definition, most data breaches do not arise from a "publication" by the policyholder. A company that is the target of a data breach has not sought to disseminate private information to the public, or to declare or announce private information publicly, which may qualify as "publication." Quite simply, "publication" is not the same thing as an alleged failure to protect information in the specific context of the coverage afforded under CGL policies. Thus, it is not surprising that the early decisions make clear that policyholders cannot rely on CGL policies to address the unique obligations and exposures posed by data breach and cyber claims.

Conclusion

Litigation over insurance coverage for costs and liabilities that policyholders face from data breaches and cyber crime will continue. To date, however, courts have signaled strongly that policyholders cannot rely on CGL coverage to address these exposures. FD