

Reproduced with permission from Privacy & Security Law Report, 15 PVLR 934, 5/9/16. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Cybersecurity Insurance

The result of *Travelers Indemnity Co. of Am. v. Portal Healthcare Solutions, LLC* is a notable win for policyholders seeking coverage for cybersecurity incidents under commercial general liability policies, the authors write.

If Information Is Available Online and No One Accesses It, Was It a ‘Publication’ for the Purpose of Insurance Coverage for Cybersecurity Loss?



BY: SERGIO F. OEHNINGER, SYED A. AHMAD AND
PATRICK M. McDERMOTT

Once in a while, interpreting an insurance policy can raise philosophical questions, such as the age-old conundrum: if a tree falls in the forest and no one hears it, does it make a sound? The recent case of *Travelers Indemnity Co. of Am. v. Portal Healthcare Solutions, LLC*, No. 14-1944, 2016 BL 112503 (4th Cir. Apr. 11, 2016) asked a similar question: if a record is

Sergio F. Oehninger is counsel in Hunton & Williams LLP's Washington office in the insurance recovery practice group.

Syed A. Ahmad is a partner in the firm's McLean, Virginia office in the insurance recovery practice group.

Patrick M. McDermott an associate in the firm's McLean, Virginia office in the insurance recovery practice group.

available online and no one sees it, does it constitute a “publication” for the purpose of insurance coverage? According to the Fourth Circuit Court of Appeals, the answer is “yes.” Affirming a federal trial court’s opinion, it ruled that the insurer must defend its insured in a class action based on the policyholder’s alleged failure to secure its server, which made medical records accessible by third parties on the Internet (15 PVLR 824, 4/18/16).

The U.S. Court of Appeals for the Fourth Circuit’s finding in *Portal* marked a notable win for policyholders seeking coverage for cybersecurity incidents under commercial general liability (CGL) policies because prior court decisions involving cybersecurity loss had found no “publication” as used in CGL policies. For example, in one prior case, a court found that there was no coverage because the relevant information was published by hackers and not by the policyholder.¹ In another case, a court concluded that there was no “publi-

¹ *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, Index No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014).

ation” where there was no suggestion that the personal information of current and former employees on lost computer tapes “was ever accessed by anyone.”²

In contrast to these decisions, the Fourth Circuit found coverage for a cybersecurity loss, deciding that there was a “publication” as used in endorsements to two CGL policies. In *Portal*, Glen Falls Hospital hired Portal Healthcare Solutions to electronically store and maintain the hospital’s confidential medical records of its patients, including hosting the records on an electronic server. Two of the hospital’s patients later found their medical records on the Internet after it conducted simple Google Inc. searches for their names. The records were available apparently as the result of a mistake on the part of Portal or the party hosting the records on an electronic server. The patients filed a class action against Portal alleging that Portal failed to safeguard the records.

The U.S. Court of Appeals for the Fourth Circuit concluded that “the medical records were published the moment they became accessible to the public via an online search.”

Portal sought coverage for this cybersecurity event under two CGL insurance policies purchased from Travelers Indemnity Company of America. Under a Web Xtend Liability Endorsement, the policies provided coverage for alleged injury arising from “electronic publication of material” that “gives unreasonable publicity to a person’s private life” or that “discloses information about a person’s private life.” Travelers sued Portal for a determination of whether the policies provided coverage.

Travelers argued that there was no publication because there was no allegation that any third party saw the records. Instead, the plaintiffs alleged only that they accessed their own records and that the information was merely *available* for access by third parties. The trial court rejected this argument. It found that publication for the purpose of insurance coverage “does not hinge on third-party access.”

The court relied on a dictionary definition of publication to determine that publication occurred “when information is ‘placed before the public,’ not when a member of the public reads the information placed before it.” It explained that, under Travelers’s logic, a book on the shelves of a bookstore isn’t actually published until someone takes the book off the shelf and reads it. To the court, this was an illogical result that didn’t comport with the plain meaning of publication. Thus, the court concluded that “the medical records were published the moment they became accessible to the public via an online search.”

Travelers offered an alternative argument that there was no “publication” because “the entire purpose of the services Portal provided was to keep the medical records private and confidential.” The court rejected this

argument, finding that the issue wasn’t whether Portal intentionally allowed the records to be accessed on the Internet. The court concluded that “an unintentional publication is still a publication.”

In cases where commercial general liability policies contain exclusions for cybersecurity-related losses, policyholders will want to procure standalone cyberinsurance coverage for such risks.

Travelers also claimed there was no “unreasonable publicity” or “disclosure” as required under the policies. Again, the court referred to dictionary definitions in refusing Travelers’s invitation to find no coverage. Publicity, according to the court, meant “the quality or state of being obvious or exposed to the general view.” There was no question that allowing medical records to be accessed online through a Google search exposed the records to the general view. Disclosure meant “the act or process of making known something that was previously unknown.” Here again, there was no question: making the medical records available made known something that was previously unknown. The court specifically rejected Travelers’s position that there was no disclosure because each record was only accessed by the corresponding patient. Like Travelers’s argument about publication, the court found that disclosure didn’t turn on whether the records were in fact accessed by third parties. Instead, they were disclosed when Portal engaged in the “process” of making known previously unknown records.

Accordingly, the trial court held that Travelers was required to provide for Portal’s defense in the class action lawsuit. On April 11, 2016, the federal appellate court affirmed the trial court’s decision, “commend[ing] the district court for its sound legal analysis.”

The *Portal* case is important in at least two respects. The court’s interpretation of the word “publication” as used in the policies can boost policyholder efforts to recover for cybersecurity-related losses under CGL policies even under policies that don’t include an endorsement similar to the Web Xtend Liability Endorsement in Portal’s policies. Coverage under the personal and advertising injury liability section of most CGL policies can be dependent on whether the loss involves an “oral or written publication.” Accordingly, the Fourth Circuit’s opinion in *Portal* should support finding a “publication” in similar circumstances under traditional CGL policies generally. However, many new CGL policies contain exclusions for cybersecurity-related losses. Those exclusions could moot the issue of whether the loss involves a “publication.” In such cases, policyholders will want to procure standalone cyberinsurance coverage for such risks.

In addition, the case is a good reminder about taking steps to secure coverage under policies of third parties like vendors. In this case, the plaintiffs in the class action sued the hospital as well as Portal. The hospital’s

² Recall *Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664, 673 (Conn. App. Ct. 2014), *aff’d*, 115 A.3d 458 (Conn. 2015).

contract with Portal could have required Portal to obtain insurance coverage for the hospital. For example, the contract could have required Portal to name the hospital as an additional insured under Portal's insurance contracts. The hospital could then attempt to recover insurance proceeds for the class action under

Portal's insurance contracts. Similar steps can help protect businesses when they are sued as the result of alleged actions or inactions of their vendors. This can be particularly important when dealing with vendors, like Portal, that are susceptible to cybersecurity losses.

This article presents the views of the authors and do not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.