KILPATRICK TOWNSEND

Insights: Alerts

General Liability Coverage for Cyber Risks Arising from "Publication" of Private Data

April 13, 2016

Written by **Caroline W. Spangenberg** and **Edmund M. Kneisel**

Cyber liability issues present constant concerns to individuals and to companies who are custodians of private data. The "hot button" issues presented range from questions regarding data theft, including identity and credit theft, to potential liability of the data custodian for such losses. Insurance carriers are marketing a variety of cyber-risk policies designed to cover such liability, including the cost of preventive measures, often mandated by state law, including the costs of notifying potential victims of loss or compromise of their private data (social security numbers, names, addresses, or personal financial information) and credit monitoring. When a large amount of private data is stolen, lost, hacked or otherwise compromised, the required, remedial costs and losses can run into the millions of dollars, even if actual, provable credit theft does not occur. Putting aside coverage specifically designed to cover such losses, courts have reached varying results when faced with claims for coverage under the "personal injury" provisions of commercial general liability (CGL) policies. Such policies typically protect against claims for invasion of privacy when private data is "published."

Courts have disagreed regarding the requirements for proof of publication of private data—is "potential" credit or identity theft enough, or must actual access to and/or misuse of the data by a third party be proven? In a potentially landmark case decided on April 11, 2016, the United States Court of Appeals for the Fourth Circuit has affirmed a ruling of a district court in Virginia holding that proof that a third party actually read and misused private data is not required to satisfy the "publication" requirement of a CGL policy. *Travelers Indem. Co. of America v. Portal Healthcare Solutions, L.L.C.*, __ Fed. Appx. ___, __ Westlaw ___, Case No. 14 1944 (4th Cir., April 11, 2016), *aff'g* , 35 F. Supp. 3d 765 (E.D. Va. 2014).

In *Portal Healthcare*, the trial court addressed the question of whether or not Travelers had a duty to defend its insured against class action claims arising out of the posting on the internet of confidential medical records, thereby "making the records available to anyone who searched for a patient's name…." 35 F. Supp.3d at 767. Travelers argued, as have other carriers in cases decided elsewhere, that there was no publication of the private data "because no third party is alleged to have viewed the information." *Id.* at 770. The trial court disagreed. The court ruled that "the issue is not whether a third party accessed the information because the definition of 'publication' does not hinge on third-party access." *Id.* at 771. Rather, citing the general, pro-insured rules of policy interpretation in Virginia (and elsewhere) when there are "uncertainties" in policy language, the court noted that the term "publication" was not defined by the policies at issue. Relying on a dictionary definition, the

court ruled that "publication" of private data occurs when private "information is 'placed before the public,' not when a member of the public reads the information placed before it." *Id.*

In reaching this result, the trial court distinguished other cases, such as *Creative Hospitality Ventures, Inc. v. U.S. Liability Ins. Co.*, 444 Fed. Appx. 370 (11th Cir. 2001) and *Recall Total Info Mgmt., Inc. v. Fed. Ins. Co.*, 147 Conn. App. 450, 83 A.3d 664 (2013), *aff'd* 317 Conn. 46, 115 A.3d 458 (2015) (per curiam) finding that no publication occurred absent proof that a third party actually read and/or misused the private data at issue. In *Creative Hospitality*, a FACTA case, the improperly disclosed credit card information was disclosed only to the credit card holder and not to any third party. In *Recall*, private data on unencrypted computer tapes had been compromised when the tapes were lost on a public highway (arguably placed before the public) and stolen by a thief. Absent evidence that the thief had read or misused any of the private data on the tapes, the Connecticut courts ruled that no publication had occurred. Distinguishing *Recall*, the *Portal Healthcare* court decided that the private medical information at issue was "given not just to a single thief but to anyone with a computer and internet access," thereby satisfying the publication requirement. The court also ruled that the public availability of the records on the internet also satisfied the policies' coverage for "unreasonable publicity" about the plaintiffs' private life because the insured had "posted their medical records on line without security restriction." *Id.* at 772. Echoing its publication ruling, the district court concluded that "the records were disclosed the moment they were posted publicly online, regardless of whether a third party viewed them." *Id.*

The Fourth Circuit's unpublished, per curiam affirmance commended the Virginia district court's "sound legal analysis." (Fourth Circuit Slip Op. p. 6). The policyholder prevailed in *Portal Healthcare*; but, in other jurisdictions, such as Connecticut, more specific allegations and proof of third party access may be necessary to establish that a "publication" of private data occurred that would to trigger a CGL policy's coverage for invasion of privacy. Nevertheless, the outcome in *Portal Healthcare* does show that in appropriate circumstances and in some jurisdictions, CGL policies can provide cyber liability protections when private data is hacked or errors by the data custodian result in the public posting of unsecured, private data on the internet.

KILPATRICK TOWNSEND

Related People

Caroline W. Spangenberg

Senior Counsel

Atlanta, GA

t 404.815.6488

cspangenberg@kilpatricktownsend.com

Edmund M. Kneisel

Retired

Atlanta, GA

t 404.815.6343

ekneisel@kilpatricktownsend.com