



# JONES DAY COMMENTARY

## DATA SECURITY, THIRD-PARTY PRIVACY CLAIMS, AND INSURANCE COVERAGE UNDER CGL “PERSONAL AND ADVERTISING INJURY” COVERAGE

*Personal and advertising injury coverage appears in standard commercial general liability (“CGL”) policies. Even though courts have been hostile to invasion of privacy claims based on data security breaches, such claims frequently are filed and are not always dismissed at an early stage. Particularly for companies that do not have specialized data security coverage, CGL coverage might provide a basis for the payment of defense costs and, if necessary, indemnity in response to such third-party claims.*

For a company faced with a data breach resulting in the possible disclosure of private information, an important question is how, if at all, commercial general liability insurance will respond to third-party claims alleging damages. If your company has specialty coverage for data security loss, cybertheft, or similar liabilities, then your right to coverage might be

clear.<sup>1</sup> If you do not have such special coverage available, however, then you might nevertheless have a prospect of recovering defense costs and indemnity under your CGL policy.

Through both inadvertence and malice, corporate entities are exposed to the risk of data security breaches that can result in the revelation of the private data pertaining to millions of customers, employees, or others. The Privacy Rights Clearinghouse estimates that more than 343 million individual records containing sensitive personal information have been involved in data security breaches in the U.S. for the period January 2005 through January

---

<sup>1</sup> The prospect of CGL coverage could, however, raise issues under an “other insurance” provision in any specialty policy.

2010. See Privacy Rights Clearinghouse, “[Chronology of Data Breaches](#).” The recent data attacks on Google and Yahoo! illustrate the way in which even the most technologically capable entities are subject to the risk that personal data of their customers can be revealed. See, e.g., *The Wall Street Journal*, “[Google Investigating If China Staff Involved in Cyber Attack](#)” (Jan. 21, 2010).

The opportunities for inadvertent loss and outright theft have grown exponentially with the ubiquity of laptops, PDA/BlackBerry devices, large-capacity microdisks, and external access to corporate systems and data. Furthermore, corporations have reported that targeted data attacks, originating from both inside and outside the entity, are on the rise. See, e.g., *Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey* (2009) (in 2009, “41% of respondents noted an increase in external attacks and 25% of respondents witnessed an increase in internal attacks.”). Moreover, the sophistication of data analysis is such that even data believed to be safely encrypted can sometimes be decoded by determined parties. See, e.g., *Valdez-Marquez, et al. v. Netflix, Inc.*, C09-05903 (N.D. Cal. 2009) (complaint filed Dec. 17, 2009) (anonymized video rental data allegedly de-anonymized and reviewed by third parties).

Just as the opportunities for security breaches escalate, legislative efforts to protect privacy rights have increased to the point of saturation. Numerous federal and state statutes now require both protection of data and notification of security breaches, meaning that customers and the public swiftly learn when a data breach occurs.<sup>2</sup> These statutes can also provide for penalties or private rights of action. In what has been reported as the first instance of state enforcement under HIPAA, the Connecticut Attorney

---

2 For example, the following statutes protect private information:

- The Personal Data Privacy & Security Act of 2007
- The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- The Gramm-Leach-Bliley Act of 1999
- The Fair Credit Reporting Act (“FCRA”)
- The Fair & Accurate Credit Transactions Act of 2003 (“FACTA”)
- The Electronic Communications Privacy Act of 1986
- The Family Educational Rights & Privacy Act (“FERPA”)
- The Video Privacy Protection Act, 18 U.S.C. § 2710

In addition, there are more than 40 state-specific laws protecting data security.

General recently sued Health Net, Inc. over an alleged failure to protect private data (and to report the breach of security) regarding more than 400,000 enrollees following the loss of a laptop computer. *Attorney General v. Health Net of the Northeast, Inc.*, D. Conn., 3:10-CV-00057-PCD (complaint filed Jan. 13, 2010).

The insurance market has responded to these risks with special coverage written to address this type of claim.<sup>3</sup> Nevertheless, for those companies with CGL insurance and no special coverage, there is an opportunity to seek coverage for defense costs (or indemnity payments, in the event of a settlement or judgment) for third-party claims under standard CGL policy wording.<sup>4</sup>

## THIRD-PARTY CLAIMS BASED ON DISCLOSURE OF PRIVATE INFORMATION

To date, courts have been somewhat hostile to claims seeking to recover damages for security breaches, rejecting them on the grounds that the plaintiffs assert only speculative loss. See, e.g., *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007) (compromise of personal information was not a “compensable injury” as required for negligence or breach of contract under Indiana law).<sup>5</sup> Nevertheless, there is no guarantee that all such claims will fail, and due

---

3 Depending on the type of conduct and harm alleged, it is possible that coverage could be provided by a specialized privacy liability policy or by E&O, commercial crime, computer crime, cyber/internet security, or other policies. Each of these coverages, if available, should be studied. This discussion focuses on standard CGL wording, but some of the concepts may be relevant under other coverages.

4 This *Commentary* does not address first-party claims, such as claims for the expense of customer notification, data retrieval and restoration, or loss of business income. A first-party claim would not be covered under CGL advertising injury coverage, although coverage could be available under specialty forms of coverage. See, e.g., *First Bank v. Federal Insurance Company*, No. 4:09-cv-00532 (Mo. Cir. Ct., March 23, 2009).

5 See also *id.* at 639 (“Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.”); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 282 (S.D.N.Y. 2008) (dismissing negligence claim based on failure to safeguard personal data when “[d]espite a full and fair opportunity to conduct discovery, there is no evidence . . . regarding the motive or capabilities of the thief . . . [and] no evidence that this plaintiff's data has been accessed or used by anyone as a result of the theft.”).

to the wide variety of common-law and statutory provisions addressing this subject, it is likely that a significant number of such claims will survive early stages of litigation and potentially proceed to final resolution.<sup>6</sup>

For example, the United States District Court for the Northern District of Illinois recently declined to dismiss a putative class action alleging violations of the Fair Credit Reporting Act and an Illinois privacy statute, along with a common-law invasion of privacy claim. *Rowe v. Unicare Life and Health Insur. Co.*, 2010 U.S. Dist. LEXIS 1576, 09-C-2286 (N.D. Ill. Jan. 10, 2010). In *Rowe*, the defendant health insurance providers advised individual plan members that some of their personal information inadvertently had been made available online to the general public. The private information included Social Security numbers, as well as medical and pharmacy information for the members and their dependents. There was no allegation that any of the information actually had been accessed or used, but simply that it had been made available online to persons who did not have the right to see it.

Among other things, the plaintiff claimed damage due to anxiety and emotional distress, an increased risk of future identity theft, and invasion of privacy. With respect to the invasion of privacy claim, the plaintiffs alleged:

As alleged herein, Defendants allowed Plaintiff's and the Class' PHI [Private Health Information] records to be published via the Internet without such persons' knowledge, authorization or consent. The publication of such private facts and information is one that is highly offensive or objectionable to a reasonable person of ordinary sensibilities. The publication of such private facts and

---

6 Data breach invasion of privacy cases are different from "blast fax" invasion of privacy cases. In a blast fax case, the information sent to the recipient/claimant typically is not the private information of the claimant, and therefore, even if there is a "publication" (usually also disputed), there is no revelation of private information to assert as a ground for coverage. *E.g.*, *Am. States Ins. Co. v. Capital Assocs. of Jackson County, Inc.*, 392 F.3d 939 (7th Cir. 2004). However, in the blast fax context, the plaintiffs can allege an invasion of their privacy right to seclusion, as opposed to the revelation of private data. *See, e.g.*, *Penzer v. Transportation Ins. Co.*, 2010 Fla. Lexis 111, No. SC08-2068 (Fla., Jan. 28, 2010) (answering question of Florida law certified from 11th Circuit, holding that liabilities for blast faxes that breached right of seclusion were covered under advertising injury coverage as "publications" of material that violated a person's right of privacy).

information does not include information which is of a legitimate public concern.

Defendants violated the rights of privacy of Plaintiff and the Class by publishing Plaintiffs and the Class' PHI records without their consent on the Internet where they were accessible to third parties.

The defendants moved to dismiss the complaint, contending that the plaintiff had not alleged injury or damage adequate to state a viable claim under any of the theories asserted. The district court denied the motion and allowed the case to proceed to discovery. In particular, the court determined that the mere "availability" of private information in a publicly accessible place (an unprotected part of the defendants' web site) might be enough to constitute a "communication" of private information for purposes of the Fair Credit Reporting Act. The court observed that, under a standard dictionary definition of "communication," if a simple expression of information is sufficient to constitute a "communication," then "the issue of whether anyone accessed the [private] information may be irrelevant." *Id.* at 4. Because the court was ruling on a motion to dismiss, it held out the possibility that, if the evidence established that private information actually was not accessed by any third party, then the FCRA claim might fail. The district court also permitted the case to proceed based largely on alleged emotional harm and an increased risk of future harm.

Addressing the common-law invasion of privacy claim, the court permitted the plaintiff to proceed based on asserted nonpecuniary harm (*i.e.*, emotional or reputational harm). The court provisionally accepted the notion that a negligent or inadvertent disclosure of protected information, even if not accessed by unauthorized persons, was a "publication" of information sufficient to allege an invasion of privacy claim under Illinois common-law.<sup>7</sup>

---

7 The court did not address the question that the defendants would not have "published" the material if they did not actually intend for the private information to be made public. This issue might still be litigated in future proceedings. For purposes of defamation, the Restatement (Second) of Torts takes the view that a completely *non-negligent* revelation of private information ordinarily will not constitute publication but suggests that a *negligent* revelation would constitute a publication. Restatement (Second) of Torts 2d § 577, cmt o.

It is likely that future statutory claims will be coupled with common-law invasion of privacy claims. A recent example is the class action lawsuit against Netflix, Inc. over customer movie rental data that allegedly could be “de-anonymized” in order to access private information. Although the complaint primarily asserts statutory claims under the Video Privacy Act and other statutes, the plaintiffs also assert a common-law breach of privacy claim. *Valdez-Marquez, et al. v. Netflix, Inc.*, C09-05903 (N.D. Cal. 2009) (filed Dec. 17, 2009).<sup>8</sup> As discussed below, claims such as these would appear to quite clearly fall within the basic CGL coverage grant for personal and advertising injury. Under the law of most jurisdictions, the defendant company therefore would be entitled to coverage of defense costs for all of the claims asserted against the company until such time as the covered claims are dismissed or, at a minimum, until there is a clear basis for allocation of defense costs among covered and noncovered claims.

## CGL COVERAGE FOR DISCLOSURE OF PRIVATE INFORMATION

The foundation for coverage under the CGL policy form is in the Side B coverage for personal and advertising injury. See, e.g., ISO CG 00 01 12 07 (“We will pay those sums that the Insured becomes legally obligated to pay as damages because of ‘personal and advertising injury’ to which this insurance applies.”). Whereas Side A coverage provides coverage for bodily injury and property damage, the “personal and advertising injury” found in Side B covers somewhat less common types of claims. In particular, the standard definition of “advertising injury” provides, in pertinent part:

14. “Personal and advertising injury” means injury, including consequential “bodily injury”, arising out of one or more of the following offenses:

\* \* \*

e. Oral or written publication, in any manner, of material that violates a person’s right of privacy . . . .

8 Plaintiffs assert: “By its conduct, Netflix has knowingly and intentionally caused the public disclosure of private facts concerning Plaintiffs and members of the U.S. Resident Class. These private facts are ones that a reasonable person would not wish disclosed and that are not newsworthy. . . . Plaintiffs and members of the U.S. Resident Class have suffered harm as a result of Netflix’s public disclosure of private facts about them.” Complaint at ¶¶ 137-139.

The CGL form does not provide a definition for “injury,” although it seems clear that the term means something more than “bodily injury,” since injury “includes” (but is not limited to) consequential bodily injury.<sup>9</sup> And, as observed by the court in *Rowe*, a plaintiff asserting a breach of privacy claim might be able to recover based on damages for emotional distress that are not linked to other bodily injury or to pecuniary loss. *Rowe*, slip op. at 16; see also *Creative Hospitality Ventures, Inc., v. United States Liability Insurance Co.*, 655 F. Supp. 2d 1613 (S.D. Fla. 2009) (“advertising injury” is different from “bodily injury” and could include a violation of one’s privacy interest in credit card information), *adopted in part, ruling reserved in part*, 655 F. Supp. 2d 1316 (S.D. Fla. 2009) (Zloch, J.).

A question likely will arise as to whether an unknowing, unintended, or inadvertent release of information—or indeed a theft of private information—can fulfill the requirement of “publication” necessary both to support a claim and to invoke coverage for the publication.<sup>10</sup> As discussed above, the *Rowe* court held in the context of a motion to dismiss that it might be satisfactory simply for the information to be *available* to the public in order for it to be “communicated” within the meaning of the FCRA.<sup>11</sup>

A federal magistrate judge for the United States District Court for the Southern District of Florida recently considered the concept of “publication” under the standard CGL wording, concluding that the phrase “publication, in any manner” is so broad that it does not require public dissemination. *Creative Hospitality Ventures, Inc. v. United States Liability Insurance Co.*, 655 F. Supp. 2d 1319 (S.D. Fla. 2009) (Rosenbaum, U.S.M.J.), *adopted in part, ruling reserved in part*, 655

9 The CGL form defines “bodily injury” as “bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time.”

10 For example, the court in *Ruiz v. Gap, Inc.*, granted a motion for judgment on the pleadings with respect to a California state constitutional breach of privacy claim on the basis that the facts underlying the breach (theft of two laptop computers) were not sufficiently egregious breaches of societal norms of conduct. 540 F. Supp. 2d 1121 (N.D. Cal. 2009). Nevertheless, until there is an adjudication that no publication or actionable breach of privacy has occurred, there is a basis to seek defense costs.

11 The concept of “communication” for FCRA purposes is not precisely the same as “publication” for invasion of privacy purposes, but it is similar enough to allow one to contend that communication constitutes publication.

F. Supp. 2d 1316 (S.D. Fla. 2009) (reserving ruling on determination that publication requirement had been fulfilled) (Zloch, U.S.D.J.). The magistrate judge observed that publication for purposes of insurance coverage is not limited to the concept of publication required for defamation, ruling that even a disclosure to the owner of the information stated a satisfactory allegation for purposes of the duty to defend and, potentially, to indemnify. *Id.* at 9–11.<sup>12</sup>

As shown by the magistrate judge’s opinion in *Creative Hospitality Ventures* opinion, tort-law definitions of “publication” do not necessarily strictly control the meaning of “publication” for purposes of insurance coverage. Nevertheless, tort law references can still be useful in making a coverage determination. For example, the Restatement (Second) of Torts provides guidance on the meaning of publication in the context of defamation law. The Restatement view is that, as long as defamatory information is revealed by way of negligence, it is sufficient to constitute publication. Restatement (Second) of Torts §577 (“Publication of defamatory matter is its communication intentionally or by a negligent act to one other than the person defamed.”). One of the examples given by the Restatement is that of a cartoonist who leaves a defamatory drawing on his desk in the middle of an office where passersby can see it. *Id.* cmt. k(5). Likewise, if an underlying claimant is able to show that a company has negligently allowed private information to be accessed by the outside world, it is likely that a strong argument for “publication” can be made.

## LIMITATIONS ON PERSONAL AND ADVERTISING INJURY

Of course, it is not enough simply to analyze the CGL coverage grant for purposes of determining whether a data breach claim might be covered. The other policy terms also must be considered.

---

<sup>12</sup> The court distinguished the decision in *Whole Enchilada, Inc. v. Travelers Prop. Cas. Co. of Am.*, 581 F. Supp. 2d 677 (W.D. Pa. 2008), in which the district court considered a different version of the personal and advertising injury wording, and concluded that the allegations and claims in the complaint did not sufficiently allege a publication that resulted in an invasion of privacy.

In particular, there is an exclusion for “knowing” violations of another’s rights.<sup>13</sup> Under the type of claim addressed here, however, the policyholder is not likely to have *knowingly* published or released the private information of the underlying claimants. Instead, the underlying cause of the breach is likely to have been negligence or theft, as in the case of a lost or stolen laptop computer. Therefore, this standard exclusion to personal and advertising injury coverage should not apply, because the policyholder would not possess the requisite advance knowledge.

Another limitation on coverage under personal and advertising injury is that the injury must be caused by an “offense” arising out of the policyholder’s business that is committed in the coverage territory during the policy period. This type of requirement ought to be readily satisfied by most data breaches. A further coverage limitation that sometimes is asserted is that the conduct creating liability must have occurred in the course of the policyholder’s “advertising.” That is, an insurer might take the position that the policy does not provide coverage unless the publication in dispute is an “advertisement.” This limitation does not, however, apply to the “invasion of privacy” coverage under the standard wording. When an invasion of privacy is asserted, the coverage responds to “oral or written publication, *in any manner*, that violates a person’s right of privacy,” and no restriction to advertising conduct exists.<sup>14</sup>

The magistrate judge in *Creative Hospitality Ventures* discussed the distinction between invasion of privacy coverage and other advertising injury. There, the insurers contended

---

<sup>13</sup> The CGL form excludes coverage for “‘Personal and advertising injury’ caused by or at the direction of the insured with the knowledge that the act would violate the rights of another and would inflict ‘personal and advertising injury.’” See ISO CG 00 01 12 07, Coverage B, Exclusion (a).

<sup>14</sup> The standard wording also contains a limiting exclusion for insureds in “Media and Internet Type Businesses.” See ISO CG 00 01 11 07, Coverage B, Exclusion (j). For this exclusion to apply, courts have sometimes considered whether the insured’s “principal” business falls within the specific language of the exclusion. See, e.g., *State Auto Prop. & Cas. Ins. Co. v. Travelers Indem. Co. of Am.*, 343 F.3d 249 (4<sup>th</sup> Cir. 2003); *American Emplrs’ Ins. Co. v. Delorme Publ’g Co.*, 39 F. Supp. 2d 64 (D. Maine 1999) (exclusion “clearly applies to insureds whose primary, essential, chief or principal business is publishing”). A policyholder faced with such an issue therefore will want to consider the case law in the relevant jurisdiction.

that publication could only occur in the context of an “advertisement.” *Id.* at 1328 n.6. The court rejected this argument, stating:

This idea does not assist the Court, however as the definition of “personal and advertising injury” does not necessarily require a covered injury to be incurred as a result of an “advertisement.” . . . Nothing in these descriptions [of covered forms of conduct and injury] requires that such injuries be incurred as the result of an “advertisement.”

*Id.*

A final exclusion that should be considered is Exclusion (p), which is entitled “Distribution of Material in Violation of Statutes.”<sup>15</sup> As it pertains to personal and advertising injury, the exclusion eliminates coverage for injury arising directly or indirectly from actual or alleged violations of the Telephone Consumer Protection Act, the CAN-SPAM Act, and other statutes, ordinances, or laws that prohibit the sending, transmitting, communicating, or distribution of material or information. This exclusion initially appeared as a stand-alone exclusion but now is incorporated into the basic policy form.<sup>16</sup> It was interpreted by the magistrate judge in *Creative Hospitality Ventures* to exclude coverage for claims under the Fair and Accurate Transaction Act, 15 U.S.C. § 1681c(g). 655 F. Supp. 2d at 1339-40.<sup>17</sup> The exclusion does not, however, purport to address common-law breach of privacy claims, and it will be a matter for litigation to determine exactly what the reach of this exclusion will be.

---

15 See ISO CG 00 01 12 07, Coverage B, Exclusion (p).

16 See ISO CG 00 67 030 05.

17 See also *Employers Mutual Casualty Company v. Witham Sales & Service, Inc.*, No. 2:08-CV-233, 2009 U.S. Dist. LEXIS 109985 (November 23, 2009) (reserving determination on exclusion’s applicability to FACTA and FCRA until necessary party could be joined).

## CONCLUSION

When a third-party claimant alleges a data security breach involving a failure to safeguard private information, a corporate insured should look not only to any specialty coverage but also to its CGL policies to see if there is a prospect of coverage. Indeed, once a data breach is known, a prudent policyholder will seek advice as to whether notice to insurers is advisable even before a claim is asserted. Any complaint is likely to assert several theories of recovery, including both statutory and common-law claims. As long as one of the asserted claims appears to involve coverage, then the policyholder may have a viable argument for reimbursement of defense costs. Moreover, if the underlying claim proceeds toward full resolution, the policyholder may also have a basis for indemnification.

## LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our “Contact Us” form, which can be found at [www.jonesday.com](http://www.jonesday.com).

### John E. Iole

+1.412.394.7914

[jeiole@jonesday.com](mailto:jeiole@jonesday.com)

### Kevin D. Lyles

+1.614.281.3821

[kdlyles@jonesday.com](mailto:kdlyles@jonesday.com)

*John Iole is a partner in Jones Day’s Insurance Recovery Practice, which is devoted to representing policyholders in all aspects of insurance coverage counseling, litigation, and alternative dispute resolution. Kevin Lyles is a Jones Day partner and is the co-chair of Jones Day’s Privacy and Data Security Practice and practice leader of the Firm’s Health Care Practice.*