# Insuring Against Privacy Claims Following A Data Breach

David J. Baldwin, Jennifer Penberthy Buckley, and D. Ryan Slaugh*

**ABSTRACT**

Companies and the lawyers who represent them are justifiably concerned about the many risks associated with cyber security threats. In today's economy, data breaches invariably result in the loss or improper disclosure of consumer data and litigation consistently ensues. Complaints frequently allege privacy-related claims, including the common law tort of unreasonable publicity given to private facts and negligence. Some jurisdictions have legislated privacy protections that either provide a statutory cause of action or can support a negligence claim. Some states and federal regulatory agencies also impose reporting obligations on companies when a data breach occurs. These consequences of a data breach represent significant expenses that should be contemplated by a company's cyber insurance strategy. Coverage may potentially be available under commercial general liability insurance, but the terms of these policies and judicial interpretation thereof increasingly preclude coverage for cyber events. The emerging market for cyber policies has resulted in diverse insurance products. Coverage under these new policies mostly remains untested in the courts. Accordingly, these products require close study to ensure that post-breach litigation is among the covered harms.

**Table of Contents**



* The authors are attorneys at Potter Anderson & Corroon LLP, which counsels and represents policyholders in coverage litigation. The opinions expressed herein are personal to the authors and are not necessarily those of Potter Anderson & Corroon LLP or its clients.

## I. INTRODUCTION

As the theme of this symposium issue of the *Penn State Law Review* suggests, business lawyers and their clients are increasingly concerned about the specter of cyber threats—and for good reason. Beyond the monetary losses, such as those resulting from the theft of valuable data or ransom required to unlock a company's systems, cyber incidents slow down business while companies recover.[1] They also lead to headlines that belie the adage, "there's no such thing as bad publicity."[2] Put simply, cyber threats are bad for business, particularly where the attack results in the loss of customers' information. But negative media coverage is not

1. *See, e.g.*, Jes Alexander, *Anatomy of a Data Breach—What Cyber Policies Should Cover*, 13 J. TEX. INS. L. 5, 12 (2015) (discussing examples of business interruption experienced by Sony following a data breach).

2. *See, e.g.*, Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could Be Affected*, CNN MONEY (Sept. 8, 2017, 9:23 AM), http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html.

the only consequence that follows exposure of consumer or other third-party data. The plaintiffs' bar is paying attention, and purported class action litigation is filed after a data breach faster than you can say "firewall."

Experience has shown that high-profile data breaches, especially those involving data the company holds on behalf of consumers, inevitably result in litigation.[3] Of the most common types of claims asserted following a data breach, among the most potentially expensive are privacy claims asserted by third parties.[4] These claims allege common law or statutory causes of action seeking damages for alleged harm caused by a company's failure to prevent the loss or theft of the plaintiffs' personal information. Often, multidistrict or class action litigation is involved.[5] In some jurisdictions, punitive damages may be available where a company has failed to comply with a statute protecting consumer information.[6] As a result, these claims are increasingly expensive to defend.[7] Businesses are faced with the distraction and expense related not only to preventing, preparing for, and responding to cyber threats, but also defending against and paying damages for privacy claims.

In view of these costs, securing insurance coverage that will respond to privacy claims is a legal and operational imperative. Developments in technology and government regulations, however, have resulted in a constantly evolving landscape that has made obtaining adequate coverage difficult.[8] Cyber threats are continually changing form as attackers develop new modes of infiltrating companies' systems. Insurers, meanwhile, have been developing a cornucopia of insurance policies, exclusions, and riders that can affect the scope of coverage.[9]

---

3. *See, e.g.*, *In re* Zappos.com, Inc., 884 F.3d 893, 895 (9th Cir. 2018) (noting that "customers responded [to notification of a data breach] almost immediately by filing putative class actions in federal district courts across the country").

4. *See, e.g.*, John Black & James R. Steel, *Privacy Developments: Private Litigation, Enforcement Actions, and Settlements*, 73 BUS. LAW. 177, 184–86 (2018).

5. *See, e.g.*, *In re* SuperValu, Inc., No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *1 (D. Minn. Mar. 7, 2018); *In re* Equifax, Inc., MDL No. 2800, 2017 WL 6031680, at *1 (J.P.M.L. Dec. 6, 2017) (noting that putative class action litigation relating to the Equifax data breach, at that time, consisted of "97 actions pending in various districts" and, in addition, that there existed "more than 200 potentially-related actions" in more than 60 district courts).

6. *See infra* Section II.A.2.

7. *See* Black & Steel, *supra* note 4, at 189 ("[T]he potential damages in privacy-related litigation are continuing to increase.").

8. *See, e.g.*, Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 371 (2015).

9. *See generally* James H. Kallianis, Jr., *Read the Fine Print: Insurance Coverage Issues Implicated in Data-Breach Claims*, 57 FOR DEF. 56 (2015).

Securing appropriate policies to ensure coverage is of critical importance. But using case law to predict coverage is a cautious enterprise, as cyber insurance policies vary significantly.[10] Although a court's reading of one contract may inform future judicial interpretation of similar provisions, each contract must be interpreted anew based on its unique terms.

This article explores strategies for insuring against the risks associated with privacy claims. First, we survey potential third-party claims that may be asserted against a company in the wake of a data breach.[11] In this discussion, we also highlight frequently litigated issues with respect to these claims in an effort to approximate the potential extent of the litigation.[12] We also consider the costs of compliance with investigations and requirements imposed by regulatory agencies, which a company's cyber insurance strategy should address. Second, we consider categories of insurance products that may respond to these claims, with particular emphasis on coverage issues that have been or may soon be litigated.[13]

## II. THE NATURE OF THE EXPOSURE

This article addresses two principal buckets of potential privacy-related losses. First, consumers who believe their personal information has been leaked or stolen in a cybersecurity incident are bringing potentially blockbuster lawsuits with increasing frequency. Understanding the differences among various privacy-related claims is necessary to grasp the scope of risks at issue. In addition, the substantive issues being litigated in this area of privacy law show the complexity of the litigation, and thereby the costs companies who are subjected to these suits can anticipate.[14] Second, a data breach may trigger regulatory agency investigations or reporting obligations.[15] These consequences represent additional costs that may not be covered by an insurer's duty to defend against litigation.

10. *Cf. The Role of Cyber Insurance in Risk Management: Hearing Before the H. Subcomm. on Cybersecurity, Infrastructure Prot., & Sec. Techs. of the H. Comm. on Homeland Sec.*, 114th Cong. 17 (2016) (statement of Adam W. Hamm, Comm'r, National Association of Insurance Comm'rs) ("[I]f you've seen [one] cybersecurity policy, you've seen exactly [one] cybersecurity policy.").

11. *See infra* Section II.A.

12. *See infra* Section II.A.

13. *See infra* Section III.

14. *See infra* Section II.A.

15. *See infra* Section II.B.

### *A. The Anatomy of Privacy Claims*

Litigation following a data breach may involve multiple privacy-related claims. This Section describes a few of the most common such claims in an effort to demonstrate the types of claims that will need to be covered by a comprehensive cyber insurance strategy.[16]

#### 1. Common Law Privacy Claims

Courts in the United States recognized privacy claims as early as the 19th century in cases involving invasions of privacy, such as eavesdropping and publishing a letter without the sender's consent.[17] Newspapers, the telephone, and instant photography assisted the development of the law in this area, as these new technologies eroded privacy in ways that led to litigation.[18] By around 1950, most states recognized a common law right to privacy.[19] As the Supreme Court of Minnesota stated when it first recognized the right:

> The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.[20]

##### a. The Tort of Invasion of Privacy

Courts generally recognize that the tort of invasion of privacy encompasses four distinct causes of action:

> (a) unreasonable intrusion upon the seclusion of another; or (b) appropriation of the other's name or likeness; or (c) unreasonable publicity given to the other's private life; or (d) publicity that unreasonably places the other in a false light before the public.[21]

16. Insurance policies may refer to invasions of the right to privacy as "advertising injuries." *See, e.g.*, Am. States Ins. Co. v. Capital Assocs. of Jackson Cty., Inc., 392 F.3d 939, 940 (7th Cir. 2004).

17. *See* Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 95 (2008).

18. *See id.* at 95–98.

19. *Id.* at 100.

20. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998).

21. Franchise Tax Bd. v. Hyatt, 407 P.3d 717, 733 (Nev. 2017) (citation omitted) (quoting RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW. INST. 1977)).

This area of the law is commonly thought of as being divided between seclusion privacy (in other words, the right to be left alone) and secrecy privacy (that is, the right to keep private information private).[22]

Giving publicity to another's private life is the invasion of privacy claim most relevant to the theft or accidental disclosure of third-party information. The information publicized must be of such a nature that its publication "would be highly offensive to a reasonable person" and "not of legitimate concern to the public."[23] Damages include harm to reputation and emotional distress.[24]

The facts at issue must be truly private; that is, the plaintiff's information cannot be of public record or a matter of public concern.[25] Nor can the plaintiff complain if someone provides a wider audience to information that the plaintiff made no effort to keep private.[26] A society increasingly willing to exchange information for convenience or entertainment may render an increasing quantity of formerly private information public.

The requirement that the publication be highly offensive to a reasonable person is an objective but relative test: that is, whether a reasonable person would be offended takes into account the customs of the community, the time period, the plaintiff's occupation, and "the habits of his neighbors and fellow citizens."[27] The reasonableness requirement is particularly thorny as society's expectation of privacy is continually evolving with new technology that makes information easier to share.[28]

---

22. *See* Am. States Ins. Co. v. Capital Assocs. of Jackson Cty., Inc., 392 F.3d 939, 941 (7th Cir. 2004). The court in *American States* explained the distinction as follows:

> A person who wants to conceal a criminal conviction, bankruptcy, or love affair from friends or business relations asserts a claim to privacy in the sense of secrecy. A person who wants to stop solicitors from ringing his doorbell and peddling vacuum cleaners at 9 p.m. asserts a claim to privacy in the sense of seclusion.

*Id.*

23. RESTATEMENT (SECOND) OF TORTS § 652D.

24. *See id.* § 652H.

25. *See, e.g.*, Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494–97 (1975) (finding unconstitutional the imposition of damages for the publication of a rape victim's name, which was public record). The Court in *Cox* further stated that "the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record." *Id.* at 494–95.

26. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. b ("[T]here is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye. Thus he normally cannot complain when his photograph is taken while he is walking down the public street and is published in the defendant's newspaper.").

27. *Id.* § 652D cmt. c.

28. *See* Sprague, *supra* note 17, at 89 ("In most cases, technology has eroded expectations of privacy—and, consequently, one's right to privacy.").

A particularly relevant element of these claims for the purposes of our discussion is the requirement of public communication of the plaintiff's personal information. "Without such disclosure to the public at large, there is no tort."[29] To be liable, the defendant must communicate the information "to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[30] Courts appear to agree that the information must at least get to a third party.[31] But what if the plaintiff's personal information is stolen from a company during a data breach? Does theft of data constitute publication of the information? Additionally, because invasion of privacy is an intentional tort, some courts have dismissed invasion of privacy claims that fail to allege an intentional act.[32] Similar questions have been implicated in judicial interpretation of insurance policies and whether they provide coverage for privacy claims.[33]

b. Negligence-Based Actions for Invasion of Privacy

The elements of a negligence claim, including negligence related to an invasion of privacy, are familiar: "It is rudimentary that in order to establish actionable negligence, one must show the existence of a duty, a breach of the duty, and an injury resulting proximately therefrom."[34] A principal concern for plaintiffs asserting a negligence claim relating to invasion of privacy is establishing that the defendant company owed a duty to safeguard the plaintiffs' data.[35] In elaborating on how to ascertain whether a defendant has a duty to a plaintiff, one court has stated:

---

29. Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1288 (N.D. Ala. 2014) (citing McNeil v. Best Buy Co., Inc., No. 4:13CV1742 JCH, 2014 WL 1316935, at *4 (E.D. Mo. Apr. 2, 2014)).

30. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a.

31. *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party."); *see also* Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 711–12 (D.C. 2009) ("Without an allegation that the data involved here were disclosed to and viewed by someone unauthorized to do so, appellants have failed to state a claim for invasion of privacy.").

32. *See Burton*, 47 F. Supp. 3d at 1288 ("Even if the defendants were negligent, as alleged, in safeguarding Mr. Burton's account information, such negligence does not morph into an intentional act of divulging his confidential information.").

33. *See infra* Sections III.A.1.b–.c (discussing cases construing the publication requirement); *infra* Section III.A.2 (discussing whether a third party must access the data and, if so, what evidence is required to demonstrate such access).

34. Menifee v. Ohio Welding Prods., Inc., 472 N.E.2d 707, 710 (Ohio 1984).

35. *Cf.* Pulka v. Edelman, 358 N.E.2d 1019, 1020–21 (N.Y. 1976). In elaborating on a defendant's duty to a plaintiff in a negligence action, the court explained:

> It is well established that before a defendant may be held liable for negligence it must be shown that the defendant owes a duty to the plaintiff. In the absence of duty, there is no breach and without a breach there is no liability. This

> In determining whether the defendant was under a duty, the court will consider several interrelated factors, including the risk, foreseeability, and likelihood of injury weighed against the social utility of the actor's conduct, the magnitude of the burden of guarding against the injury, and the consequences of placing the burden on the defendant.[36]

Common law principles of duty have been held not to support a cause of action for negligence following a data breach: normally, the "holder of personal data may have no general duty of care, and even sensitive data does not automatically create a special trust-based or fiduciary duty."[37] Additionally, courts view with disfavor efforts to hold a party liable for the criminal acts of third parties.[38] Exceptions exist, however, as noted by the Second Restatement of Torts:

> In general, these [exceptions exist] where the actor is under a special responsibility toward the one who suffers the harm, which includes the duty to protect him against such intentional misconduct; or where the actor's own affirmative act has created or exposed the other to a recognizable high degree of risk of harm through such misconduct, which a reasonable man would take into account.[39]

Duty also may be based on violation of a statute.[40] Additionally, courts look to statutes to provide the applicable standard of care if the statute's purpose is:

---

> requirement is expressed in the often-quoted remark: 'Negligence in the air, so to speak, will not do.'

*Id.* (citations omitted).

36. Greater Hous. Transp. Co. v. Phillips, 801 S.W.2d 523, 525 (Tex. 1990); *see also* Snyder v. Med. Serv. Corp. of E. Wash., 35 P.3d 1158, 1164 (Wash. 2001) ("The existence of a duty is a question of law and depends on mixed considerations of 'logic, common sense, justice, policy, and precedent.'" (citation omitted)).

37. David L. Silverman, *Developments in Data Security Breach Liability*, 73 BUS. LAW. 215, 222 (2018) (citing cases).

38. *See, e.g.*, Veridian Credit Union v. Eddie Bauer, LLC, No. C17-0356JLR, 2017 WL 5194975, at *9 (W.D. Wash. Nov. 9, 2017) ("[A]n actor ordinarily owes no duty to protect an injured party from harm caused by the criminal acts of third parties." (quoting Parrilla v. King Cty., 157 P.3d 879, 884 (Wash. Ct. App. 2007))).

39. RESTATEMENT (SECOND) OF TORTS § 302B cmt. e (AM. LAW. INST. 1965).

40. *See Veridian*, 2017 WL 5194975, at *9 ("'Duty in a negligence action is a threshold question' and 'may be predicated on violation of statute or of common law principles of negligence.'" (quoting Jackson v. City of Seattle, 244 P.3d 425, 428 (Wash. Ct. App. 2010))); *cf.* RESTATEMENT (SECOND) OF TORTS § 874A (1979). The Second Restatement of Torts suggests that tort liability is appropriate in certain instances of violations of legislative provisions:

> When a legislative provision protects a class of persons by proscribing or requiring certain conduct but does not provide a civil remedy for the violation, the court may, if it determines that the remedy is appropriate in furtherance of the purpose of the legislation and needed to assure the effectiveness of the provision, accord to an injured member of the class a right of action, using a

> (a) to protect a class of persons which includes the one whose interest is invaded, and
>
> (b) to protect the particular interest which is invaded, and
>
> (c) to protect that interest against the kind of harm which has resulted, and
>
> (d) to protect that interest against the particular hazard from which the harm results.[41]

A recent case from the United States District Court for the Western District of Washington, *Veridian Credit Union v. Eddie Bauer, LLC*,[42] illustrates the intersection between statutes related to data security and negligence claims related to data breaches. Following a data breach in which hackers installed malware on computers in Eddie Bauer, LLC ("Eddie Bauer") stores that stole consumer credit and debit card information, Veridian Credit Union ("Veridian"), an issuer of payment cards that were compromised in the breach, asserted a putative class action against Eddie Bauer, alleging negligence, negligence *per se*, and violation of Washington statutes[43] "address[ing] unauthorized cyber-intrusions on the account information of credit card and debit card holders."[44]

On Eddie Bauer's motion to dismiss, the court quickly dispensed with the negligence *per se* claim because, in Washington, violation of a statute constitutes only evidence of negligence and not a separate cause of action.[45] The court next considered whether Eddie Bauer owed a duty to safeguard Veridian's customer data. The court determined that no duty exists under the common law for Eddie Bauer to prevent the criminal act of a third party, reasoning that there existed no special relationship between Eddie Bauer and Veridian and the complaint alleged only omissions (i.e., no affirmative act that placed Veridian in a position of peril).[46]

Veridian also alleged, however, that Eddie Bauer owed it a duty based on two legislative efforts: the Federal Trade Commission Act of

---

> suitable existing tort action or a new cause of action analogous to an existing tort action.

RESTATEMENT (SECOND) OF TORTS § 874A.

41. RESTATEMENT (SECOND) OF TORTS § 286 (1965).

42. Veridian Credit Union v. Eddie Bauer, LLC, No. C17-0356JLR, 2017 WL 5194975 (W.D. Wash. Nov. 9, 2017).

43. *See id.* at *1–2.

44. *Id.* at *5.

45. *See id.* at *8.

46. *See id.* at *9–10.

1914[47] (FTCA) and Washington Revised Code Section 19.255.020,[48] the latter of which the court described as "designed to address damage to financial institutions from the unauthorized cyber-intrusions of the account information of credit card and debit card holders."[49] The court rejected Veridian's argument that the FTCA imposed a duty on Eddie Bauer, reasoning that the FTCA was designed to prevent the destruction of competition, which had not been alleged by Veridian.[50] The Washington statute, on the other hand, was specifically designed to protect against harms alleged by Veridian.[51] Accordingly, the court permitted Veridian's negligence claim to proceed because the Washington statute established a duty and standard of care applicable to the action.[52]

In addition to duty based on statutory violations such as the one recognized in *Eddie Bauer*, some courts have recognized a duty to safeguard data based on contract[53] or the existence of an employment

47. Federal Trade Commission Act of 1914, ch. 311, 38 Stat. 717 (codified as amended at 15 U.S.C. § 45 (2012)).

48. WASH. REV. CODE § 19.255.020 (2018).

49. *Veridian*, 2017 WL 5194975, at *10.

50. *Id.* ("Section 5 of the [FTCA] is not designed to protect either the class of persons that includes Veridian or the interest that Veridian alleges Eddie Bauer invaded.").

51. *Id.* at *11. The court stated:

> The "class of persons" that this statute is designed to protect is comprised of "financial institution[s]" that have incurred "actual costs" related to the unauthorized access of their credit card and debit card holders' account information. Veridian and its putative class of similarly situated financial institutions fall within this "class of persons." In addition, the particular interest which the statute seeks to protect—the security of the financial institutions' credit card and debit card holders' account information—is the same interest that would be protected by imposing a duty on Eddie Bauer with respect to Veridian's negligence claim. Finally, the harm or hazard that a violation of [Washington Revised Code Section] 19.255.020 causes—actual costs due to the unauthorized access of account holders' information—is the same as the harm alleged by Veridian in its negligence claim. Accordingly, the court finds that [Washington Revised Code Section] 19.255.020 meets the test set forth in Section 286 of the Restatement.

*Id.* (first alteration in original) (citation omitted).

52. *See id.* at *12 ("[T]he 'reasonable care' standard found in [Washington Revised Code Section] 19.255.020 defines the minimum standard of conduct under Washington law for processors or businesses whose alleged failure to protect from unauthorized access credit and debit card account information that is in their possession causes damage to financial institutions.").

53. *See* Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 760 (W.D.N.Y. 2017) (describing a situation in which a privacy policy was potentially incorporated by reference into a health plan agreement with subscribers, giving rise to contractual duty to conform to privacy policy in order to protect subscriber data).

relationship between the defendant and plaintiff-employees.[54]

Because a duty may be predicated on state law, early stages of litigation over statutory claims may focus on the appropriate choice of law, with the defendant hoping to avoid application of the law of states such as Washington, while plaintiffs seek the opposite. In the *Eddie Bauer* litigation described above, Eddie Bauer contended that Iowa law should apply, arguing that the harm occurred in Iowa because Veridian was an Iowa-chartered credit union.[55] Veridian sought application of Washington law.[56] Applying Washington choice of law principles,[57] the court decided that Washington law applied because it had the most significant relationship to the action.[58] The court rejected Eddie Bauer's argument that the place of the conduct causing the injury was "unknown" because the hackers were unidentified, reasoning that:

> Veridian is not suing the cyber attacker. Veridian is suing Eddie Bauer for negligence and other misconduct related to its management's decisions concerning Eddie Bauer's internal data security and the Data Breach. Veridian alleges that Eddie Bauer "orchestrated and implemented" the decisions that lead [sic] to the Data Breach "at its corporate headquarters in Bellevue, Washington," and its failure to employ adequate data security measures "emanated from [its] headquarters." Based on these allegations, the court concludes that the place where the conduct alleged to have caused the injury occurred was in Washington.[59]

The court also emphasized that Washington had the greater interest in adjudicating the action because of the statutory claims alleged:

> Washington has the paramount interest in applying its law to this action. In addition to its negligence claims, Veridian also asserts claims based on [Washington Revised Code Section] 19.255.020, which is designed to fight unauthorized cyber-intrusions into credit card and debit card holders' data, and the CPA [(Consumer Protection Act)]. The CPA targets all unfair trade practices either originating from Washington businesses or harming Washington citizens. Application of

54. *See* Savidge v. Pharm-Save, Inc., No. 3:17-CV-00186-TBR, 2017 WL 5986972, at *3 (W.D. Ky. Dec. 1, 2017) (referring to defendant employer's duty to safeguard employees' personal and sensitive information, but concluding that the employees' allegations concerning alleged injury were insufficient); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 747–49 (S.D.N.Y. 2017) (recognizing a common law and statutory duty to safeguard employee data).

55. *See Veridian*, 2017 WL 5194975, at *2–3.

56. *Id.* at *3.

57. *Id.* ("A 'federal court sitting in diversity ordinarily must follow the choice-of-law rules of the State in which it sits.'" (citation omitted)).

58. *See id.* at *5–8.

59. *Id.* at *6 (citations omitted).

> the CPA to Veridian's claims effectuates the broad deterrent purpose of CPA, especially as applied to one of Washington's leading corporate citizens. The same is true of [Washington Revised Code Section] 19.255.020, which applies to credit card processors and businesses, rendering them potentially liable to financial institutions if they fail to "take reasonable care to guard against unauthorized access to account information." Thus, the court concludes that Washington law applies to this action . . . .[60]

Although Eddie Bauer did not prevail on its choice of law argument, the analysis is case specific. Companies facing privacy claims should not be deterred from considering a similar approach early in the litigation. A favorable ruling on this issue may limit the scope of a case. Not only may it eliminate claims based on violations of state statutes, but also it can undercut a plaintiff's negligence claims where duty or the standard of care is predicated on violation of state law.

c. Article III Standing: The Injury-in-Fact Requirement

A frequently litigated issue in privacy-related cases is whether the plaintiff has standing to pursue the claim. Federal courts lack subject matter jurisdiction over a case unless the plaintiff can satisfy the requirements of Article III of the United States Constitution.[61] "To meet the requirements of Article III standing, a plaintiff must establish that he has suffered an injury in fact, that the injury was causally connected to the defendant's actions, and that a judgment in the plaintiff's favor will redress the injury."[62] To establish injury in fact, the plaintiff must demonstrate that he or she has suffered "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not "conjectural" or "hypothetical."'"[63]

The United States Supreme Court addressed the injury-in-fact requirement in the digital world in *Spokeo, Inc. v. Robins*.[64] There, the plaintiff, Thomas Robins ("Robins") initiated a purported class action

60. *Id.* at *8 (citations omitted).

61. *See, e.g.*, Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

62. Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1282 (N.D. Ala. 2014) (citing Koziara v. City of Casselberry, 392 F.3d 1302, 1304 (11th Cir. 2004)).

63. *Lujan*, 504 U.S. at 560 (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)); *see also In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 24 (D.D.C. 2014) ("Allegations of possible future injury do not satisfy the requirements of Art[icle] III. A threatened injury must be *certainly impending* to constitute injury in fact." (quoting *Whitmore*, 495 U.S. at 158)). A purported class action plaintiff must meet this burden without resorting to facts that can be alleged by other members of the purported class. *See* Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 40 n.20 (1976) (citing Warth v. Seldin, 422 U.S. 490, 511 (1975)).

64. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (7-2 decision).

under the Fair Credit Reporting Act[65] (FCRA) against Spokeo, Inc. ("Spokeo"), an online "people search engine[,]"[66] after he discovered that Spokeo had "gathered and then disseminated" incorrect information about him.[67] The trial court concluded that Robins had failed to plead an injury in fact and dismissed the case for lack of standing.[68] The United States Court of Appeals for the Ninth Circuit reversed, reasoning that Robins had alleged a violation of his statutory rights and harm to his "personal interests in the handling of his credit information."[69] A seven-Justice majority of the United States Supreme Court determined that the Ninth Circuit erred by failing to consider whether Robins alleged "an injury that is both 'concrete *and* particularized.'"[70] The Court remanded for the Ninth Circuit to decide whether Robins's allegations were sufficiently concrete.[71]

In its decision, the Court in *Spokeo* discussed the concreteness and particularity requirements in the context of intangible injuries.[72] Although the Court often looks to Congress for guidance on which intangible harms are sufficiently concrete for standing purposes,[73] the Court clarified that "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[74] Thus, "a bare procedural violation, divorced from any concrete

65. 15 U.S.C. § 1681 (2012).

66. *See Spokeo*, 136 S. Ct. at 1544. In elaborating on the underlying nature of Spokeo's business, the court stated:

> [Spokeo] operates a Web site that allows users to search for information about other individuals by name, e-mail address, or phone number. In response to an inquiry submitted online, Spokeo searches a wide spectrum of databases and gathers and provides information such as the individual's address, phone number, marital status, approximate age, occupation, hobbies, finances, shopping habits, and musical preferences.

*Id.* at 1546. The Court assumed for the purposes of the appeal that Spokeo was a consumer reporting agency subject to the FCRA. *Id.* at 1546 n.4.

67. *Id.* at 1544.

68. *See id.* at 1546.

69. *Id.* (quoting Robins v. Spokeo, Inc., 742 F.3d 409, 413 (9th Cir. 2014)).

70. *Id.* at 1545 (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180 (2000)).

71. *See id.* The dissenting Justices generally agreed with the majority's analysis, but opined that remand was not necessary because, in their view, Robins had pled sufficient facts to demonstrate that his injury was sufficiently concrete. *See id.* at 1555 (Ginsburg, J., dissenting).

72. *See id.* at 1549 (majority opinion).

73. *See id.* ("Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before." (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring in part and concurring in judgment))).

74. *Id.*

harm," fails to "satisfy the injury-in-fact requirement of Article III."[75] The "risk of real harm"[76] identified by Congress, however, may be sufficient in some circumstances to establish standing, such as where plaintiffs have been denied access to information that Congress decided to make public.[77] Although the Court did not decide whether a bare violation of FCRA satisfied the injury-in-fact requirement, the majority observed that it was "difficult to imagine" how minor inaccuracies in an individual's credit report, without more, would "present any material risk of harm."[78]

Courts have recognized that pleading sufficient facts to demonstrate standing in data breach cases is challenging.[79] Part of the difficulty is that the law is unclear regarding when a cognizable injury has occurred following a data breach. Courts generally recognize that actual theft of a plaintiff's identity is sufficient.[80] What is less clear is whether that degree of harm is required. As phrased by one court, "when is a consumer actually harmed by a data breach—the moment data is lost or stolen, or only after the data has been accessed or used by a third party?"[81]

Generally, plaintiffs must plead facts beyond the data breach itself.[82] Some plaintiffs have attempted to meet this burden by pointing to an increased risk of future injury, such as identity theft.[83] "An allegation of future injury may suffice if the threatened injury is 'certainly

---

75. *Id.* (citing Summers v. Earth Island Inst., 555 U.S. 488, 496 (2009); *Lujan*, 504 U.S. at 572).

76. *Spokeo*, 136 S. Ct. at 1549.

77. *See id.* at 1549–50 (citing Fed. Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998); Pub. Citizen v. U.S. Dep't of Justice, 491 U.S. 440, 449 (1989)).

78. *Id.* at 1550.

79. *See* Burton v. MAPCO Express, 47 F. Supp. 3d 1279, 1280 (N.D. Ala. 2014). In *Burton*, the court observed that:

> [I]t is difficult for consumers . . . to assert a viable cause of action stemming from a data breach because in the early stages of an action, it is challenging for a consumer to plead facts that connect the dots between the data breach and an actual injury so as to establish Article III standing [and permitting the plaintiff to re-plead because] litigation relating to computer data breaches is a relatively new phenomenon, and the law in this area is developing fairly quickly . . . .

*Id.* at 1280.

80. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017) ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."), *cert. denied*, 138 S. Ct. 981 (2018).

81. *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 19 (D.D.C. 2014).

82. *See id.*

83. *See, e.g.*, *Attias*, 865 F.3d at 628 (involving plaintiffs who alleged a "material risk of identity theft" resulting from the theft of names, dates of birth, social security numbers, and credit card numbers (quoting Second Amended Complaint at 8, *Attias*, 865 F.3d 620 (No. 16-7108))).

impending,' or there is a 'substantial risk' that the harm will occur."[84] The United States Court of Appeals for the District of Columbia Circuit has developed a framework for analyzing when these standards are met in data breach cases, which "'consider[s] the ultimate alleged harm,' which in this case would be identity theft, 'as the concrete and particularized injury and then . . . determine[s] whether the increased risk of such harm makes injury to an individual citizen sufficiently "imminent" for standing purposes.'"[85]

Plaintiffs have attempted to establish injury in fact by alleging that they purchased identity theft protection to protect themselves from harm that might result from the data breach.[86] In *Clapper v. Amnesty International USA*,[87] the United States Supreme Court considered whether the injury-in-fact requirement was met where lawyers and others went to additional expense to alleviate their fear of being subject to surveillance under the Foreign Intelligence Surveillance Act[88] when they communicated with individuals outside the United States.[89] The Court stated that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[90] Some courts have applied this statement from *Clapper* by analogy to plaintiffs in data breach cases to conclude that the "cost of credit monitoring and other preventive measures . . . cannot create standing."[91] The Court's standing analysis in *Clapper*, however, was much broader than its statement about manufactured standing. The Court concluded that the plaintiffs' allegations were too attenuated:

> [R]espondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under [50 U.S.C] § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with

84. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)).

85. *Attias*, 865 F.3d at 627 (quoting Food & Water Watch, Inc. v. Vilsack, 808 F.3d 905, 915 (2015)).

86. *See, e.g.*, *In re Sci. Applications*, 45 F. Supp. 3d at 26.

87. Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

88. Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–46, 1861–1862, 1871).

89. *See Clapper*, 568 U.S. at 415–16.

90. *Id.* at 416.

91. *In re Sci. Applications*, 45 F. Supp. 3d at 26.

> the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts. As discussed below, respondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.[92]

Additionally, the Ninth Circuit later suggested that "*Clapper*'s standing analysis was 'especially rigorous' because the case arose in a sensitive national security context involving intelligence gathering and foreign affairs, and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional."[93]

Accordingly, while *Clapper* for a time may have been the best data point available to trial courts concerning whether purchasing identity theft protection constituted concrete and particularized harm, it probably is not accurate to say that paying for identity theft protection can never create standing. Indeed, some courts, distinguishing *Clapper*, have determined that the increased risk of identity theft alone is sufficient to establish injury in fact, at least at the pleading stage.[94] Where a plaintiff alleges that his or her personal information has been stolen by a hacker, the injury does "not require a speculative multi-link chain of inferences" if the hacker has "all the information . . . needed to open accounts or spend money in the plaintiffs' names."[95]

From the above cases, a few general principles can be distilled. Theft of personal data by a hacker that gives rise to an increased risk of identity theft generally is sufficient to establish injury in fact.[96] The type

---

92. *Clapper*, 568 U.S. at 410 (citations omitted).

93. *In re* Zappos.com, Inc., 884 F.3d 893, 897 (9th Cir. 2018) (quoting *Clapper*, 568 U.S. at 408).

94. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018). The Court in *Attias* stated:

> No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken. That risk is much more substantial than the risk presented to the *Clapper* Court, and satisfies the requirement of an injury in fact.

*Id.*

95. *In re Zappos.com*, 884 F.3d at 897.

96. *See, e.g.*, *Attias*, 865 F.3d at 628 ("[Where] an unauthorized party has already accessed personally identifying data . . . it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill."); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (finding that "continuing, increased risk" of identity theft constitutes sufficient injury); *cf.* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Presumably,

of data stolen, however, will inform whether the risk of future injury is sufficient. The theft of a credit card number alone, for example, has been determined to be insufficient.[97] But the theft of any information with which a criminal can commit identity theft is sufficient, even if the complaint does not allege theft of social security numbers.[98]

2. Statutory Privacy Claims

The availability of statutory causes of action relating to privacy claims raises the stakes for companies that suffer a data breach. These claims may provide for fee shifting or other penalties.[99] In some states, allegations of statutory violations may support a plaintiff's ability to establish the duty or breach elements of a negligence claim.[100] Additionally, a statutory violation may result in denial of coverage if the relevant policy provisions exclude coverage for unlawful acts.[101]

a. Fair Credit Reporting Act Claims

Congress enacted the FCRA in recognition of "a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[102] Thus, the FCRA "require[s] that consumer reporting

---

the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

97. *See* Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc., Customer Data Sec. Breach Litig.), 870 F.3d 763, 769–70 (8th Cir. 2017) (noting that the complaint alleged theft only of credit card information, which a report cited in the plaintiffs' complaint indicated "generally cannot be used alone to open unauthorized new accounts" (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 30 (2007))).

98. *See In re Zappos.com*, 884 F.3d at 899 (noting that the information alleged to have been stolen constituted sufficient "means to commit fraud or identity theft," such as by phishing or pharming, which the defendant had "effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used" a similar password).

99. *See, e.g.*, 15 U.S.C. § 1681n (2012).

100. *See supra* Section II.A.1.b (discussing negligence-based actions for invasion of privacy).

101. *See infra* Section III.A.1.a (discussing one such case).

102. 15 U.S.C. § 1681(a)(4); *cf. id.* § 1681a(c) ("The term 'consumer' means an individual."); *id.* § 1681a(f). Section 1681a(f) of Title 15 of the U.S. Code provides the following definition:

> The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[103] Specifically, the FCRA provides that "[e]very consumer reporting agency shall maintain reasonable procedures designed . . . to limit the furnishing of consumer reports to the purposes listed under section 1681b of this title."[104] It also imposes requirements on companies who: (1) use information retrieved from credit reporting agencies; and (2) deliver information (such as that relating to delinquent accounts) to credit reporting agencies.[105] "Enacted long before the advent of the Internet, the FCRA applies to companies that regularly disseminate information bearing on an individual's 'credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.'"[106]

The FCRA includes enforcement provisions for willful[107] and negligent noncompliance.[108] A finding of willful noncompliance may result in attorney's fees and punitive damages.[109] Actions must be brought in any United States district court within two years of the plaintiff's discovery of the violation or five years after the date the violation occurred, whichever occurs sooner.[110]

b. Illinois's Biometric Information Privacy Act

Illinois has taken the unique step of adopting its Biometric Information Privacy Act[111] (BIPA), which requires companies to protect biometric identifiers, such as fingerprints and face scans.[112] Specifically, when companies "collect or purchase biometric identifiers," those companies must "first (1) inform subjects that the information is being collected or stored; (2) inform subjects of the purpose and length of term for which the information is being collected and stored; and (3) receive

---

*Id.* § 1681a(f).

103. *Id.* § 1681(b).

104. *Id.* § 1681e(a).

105. *See id.* §§ 1681m, 1681s-2.

106. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016) (quoting 15 U.S.C. § 1681a(d)(1)).

107. 15 U.S.C. § 1681n.

108. *Id.* § 1681o.

109. *Id.* § 1681n.

110. *Id.* § 1681p.

111. 740 ILL. COMP. STAT. 14/1 (2018).

112. *See* 740 ILL. COMP. STAT. 14/15(e); *see also* Erin Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies*, 73 BUS. LAW. 191, 192 (2018).

from subjects written consent to collect the information."[113] Companies must also use "the reasonable standard of care" applicable to their industry to protect this information.[114] The statute also confers a private right of action on affected individuals, with penalties of $1,000 for each negligent occurrence and $5,000 for each intentional or reckless occurrence.[115] An intermediate appellate court in Illinois has narrowed BIPA somewhat by concluding that "a 'person aggrieved' by . . . a violation must allege some actual harm."[116]

c. State Consumer Protection Statutes

State legislatures are increasingly concerned with the potential public harm of data breaches, as evidenced by the legislative activity in this area.[117] The Washington statute at issue in the *Eddie Bauer* case, discussed earlier,[118] is one example.[119] Under that provision, the following applies:

> If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the

113. Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 4.

114. *Id.* (quoting 740 ILL. COMP. STAT. 14/15(e)).

115. *See* 740 ILL. COMP. STAT. 14/20(1)–(2) ("Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.").

116. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 1.

117. For a summary of legislative activity relating to data security, see *Cybersecurity Legislation 2017*, NAT'L CONF. ST. LEGISLATURES (Dec. 29, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx. Although legislative efforts in this area have primarily occurred at the state level, in October 2017 the United States House of Representatives introduced the Consumer Privacy Protection Act of 2017. As of March 6, 2018, no action has been taken on the bill. *All Information (Except Text) for H.R. 4081 - Consumer Privacy Protection Act of 2017*, CONGRESS, https://www.congress.gov/bill/115th-congress/house-bill/4081/all-info (last visited Mar. 6, 2018). Experience teaches that this bill is not likely to go anywhere. *See* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating A Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 615–16 (2018) ("Proposals generally rise, then stall, within a familiar cycle of (1) major breach; (2) introduction of one or more data security bills; and (3) legislative inaction.").

118. *See supra* Section II.A.1.b.

119. WASH. REV. CODE § 19.255.020 (2017).

> financial institution has not suffered a physical injury in connection with the breach.[120]

Washington provides for mandatory attorneys' fees.[121] Similarly, effective April 14, 2018, Delaware requires those who do business in the state to implement reasonable protections for consumer data.[122]

In a carrot-and-stick approach, Washington also provides for a safe harbor for companies that implement encryption programs or take other recognized steps to safeguard consumer data. Specifically, Washington protects companies from liability where "(a) the account information was encrypted at the time of the breach, or (b) the processor, business, or vendor was certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach."[123]

Many of these provisions also impose reporting obligations on companies that suffer a data breach.[124] The vast majority of states have adopted disclosure requirements in some form.[125] Some states also require disclosure to credit reporting agencies once the extent of the breach reaches a certain threshold of individuals affected.[126] Companies may also be required to offer free credit monitoring services for affected consumers.[127]

---

120. *Id.* § 19.255.020(3)(a).

121. *See id.*

122. *See* DEL. CODE ANN. tit. 6, § 12B-100 (West 2018) (effective Apr. 14, 2018) ("Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.").

123. WASH. REV. CODE § 19.255.020.

124. *See, e.g.*, WASH. REV. CODE § 19.255.010. The Washington Revised Code states, in relevant part:

> [C]ompanies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured.

*Id.*

125. *See, e.g.*, IND. CODE § 24-4.9-3-1(a), (c) (2018) (requiring reporting to consumers and to the Indiana attorney general); WASH. REV. CODE § 19.255.010(1). For a full list of the data breach reporting legislation, see the comprehensive data assembled by the National Conference of State Legislatures. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

126. *See, e.g.*, IND. CODE § 24-4.9-3-1(b) (requiring such reporting when over 1,000 Indiana consumers are affected).

127. *See, e.g.*, DEL. CODE ANN. tit. 6, § 12B-102(e). The Delaware Code provides, in relevant part:

> If the breach of security includes a Social Security number, the person shall offer to each resident, whose personal information, including Social Security

Although enforcement mechanisms for many of these statutes exist, some courts have determined with respect to some of these statutes that only the state attorney general may bring an action and that no private right of action exists.[128] Some state courts have concluded that the relevant state statute sets a standard of care sufficient to give rise to a negligence cause of action where a company permits consumer data to be stolen or leaked.[129]

### *B. Responding to Government Investigations and Enforcement Actions*

Companies who suffer a data breach may soon find themselves faced with a government investigation. Unfortunately, even insurance that covers formal proceedings before regulatory agencies may not cover the more informal aspects of regulatory investigations.[130]

Some industries may be more likely to be subject to scrutiny.[131] The healthcare industry, for example, is subject to heightened regulations. The Health Insurance Portability and Accountability Act[132] (HIPAA), amended by the American Recovery and Reinvestment Act,[133] mandates prompt notification of a data breach and includes penalties for failure to

---

number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. Such person shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file. Such services are not required if, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

*Id.*

128. *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 977 (N.D. Cal. 2016) ("Indiana's data breach statutes continue to provide a single enforcement mechanism: an action brought by the state Attorney General.").

129. *See supra* Section II.A.1.b (discussing negligence-based actions for invasion of privacy).

130. *See* John G. Buchanan & Marialuisa S. Gallozzi, *Kicking the Tires On a New Cyber Policy: Top Tips and Traps*, ABA SEC. LITIG., COMMITTEE ON INS. COVERAGE (Jan. 22, 2018), https://www.americanbar.org/groups/litigation/committees/insurance-coverage/articles/2017/cyber-policy-tips-traps.html.

131. For an argument that such industries should be required to carry cyber liability insurance as a way to effectively outsource regulation, see Minhquang N. Trang, Note, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches*, 18 MINN. J.L. SCI. & TECH. 389, 409–16 (2017).

132. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

133. *See, e.g.*, American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402, 123 Stat. 115, 260 (codified as amended at 42 U.S.C. § 17932 (2012)).

do so.[134] The United States Department of Health and Human Services has been willing to enforce these reporting requirements with vigor.[135]

The Federal Trade Commission (FTC) is one government agency that historically has aggressively investigated and prosecuted companies who have allegedly failed to safeguard consumer data.[136] The FTC gets its authority from the FTCA, which permits the FTC to prevent "unfair or deceptive acts or practices in or affecting commerce."[137] An act or practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[138]

A recent appeal to the United States Court of Appeals for the Eleventh Circuit suggests that judicial intervention may soon curtail the FTC's authority.[139] In *LabMD, Inc. v. Federal Trade Commission*, the Eleventh Circuit granted a stay pending appeal from the FTC's determination that LabMD had engaged in unfair practices after one of its employees downloaded a peer-to-peer file-sharing application to a LabMD computer that could have permitted a third party to access patient information stored on her computer.[140] The court stated that the FTC's interpretation of the FTCA was entitled to *Chevron, U.S.A., Inc. v.*

134. *See* 42 U.S.C. § 17932; 45 C.F.R. §§ 164.400–.414 (2018).

135. *See, e.g.*, *Failure to Protect the Health Records of Millions of Persons Costs Entity Millions of Dollars*, U.S. DEP'T HEATH & HUM. SERVS. (Dec. 28, 2017), https://www.hhs.gov/about/news/2017/12/28/failure-to-protect-the-health-records-of-millions-of-persons-costs-entity-millions-of-dollars.html; *First HIPAA Enforcement Action for Lack of Timely Breach Notification Settles for $475,000*, U.S. DEP'T HEATH & HUM. SERVS. (Jan. 9, 2017), http://wayback.archive-it.org/3926/20170127111957/https:/www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html.

136. *See, e.g.*, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, FED. TRADE COMMISSION (Jan. 6, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million; *Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That It Violated Financial Privacy and Security Rules*, FED. TRADE COMMISSION (Aug. 29, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges; *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk*, FED. TRADE COMMISSION (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment; *cf.* Black & Steel, *supra* note 4, at 181 (describing the FTC's "aggressive enforcement").

137. 15 U.S.C. § 45(a) (2012).

138. *Id.* § 45(n).

139. *See* LabMD, Inc. v. Fed. Trade Comm'n, 678 F. App'x 816, 817 (11th Cir. 2016).

140. *See id.* at 818.

*Natural Resources Defense Council, Inc.*[141] deference—if reasonable.[142] But it agreed with LabMD that "there are compelling reasons why the FTC's interpretation may not be reasonable," citing the lack of tangible harm and any evidence that patient information was actually accessed by a third party.[143] Although the court's decision on the merits has yet to issue, this discussion in the court's order granting the motion to stay casts some doubt on the FTC's ability to dictate privacy practices[144] to companies that have not acted in a manner likely to harm consumers.

Additionally, under the Trump administration, the FTC has been undergoing a transition period. A recent speech delivered by Acting FTC Chairman Maureen K. Ohlhausen may suggest that the FTC's new leadership intends to focus less on the LabMDs of the world and more on companies that cause actual harm to consumers.[145] In September 2017, Ms. Ohlhausen stated that it was "plain good policy" to focus on consumer injuries: "Government does the most good with the fewest unintended side effects when it focuses on stopping substantial consumer injury instead of expending resources to prevent hypothetical injuries."[146]

The Federal Bureau of Investigation (FBI) has also indicated that it will view companies that experience data breaches more sympathetically.[147] On March 7, 2018, FBI Director Christopher Wray stated at a cybersecurity conference that his bureau intended to "treat victim companies as victims" and assured the private sector that, absent a court order, the FBI would not be inclined to pass company information

141. Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 842–43 (1984).

142. *LabMD*, 678 F. App'x at 820 (citing *Chevron*, 467 U.S. at 842–43 (1984)). *See generally* William N. Eskridge, Jr. & Lauren E. Baer, *The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations from* Chevron *to* Hamdan, 96 GEO. L.J. 1083 (2008) (explaining *Chevron* deference as it relates to other judicial standards of review).

143. *See LabMD*, 678 F. App'x at 820–21.

144. The FTC ordered LabMD to "implement a number of compliance measures including creating a comprehensive information security program; undergoing routine professional assessments of that program; providing notice to any possible affected individual and health insurance company; and setting up a toll-free hotline for any affected person to call." *Id.* at 821. The court concluded that being forced to comply with the FTC's order pending the appeal would cause irreparable harm to LabMD, which went out of business as a result of costs associated with the FTC proceedings thus far. *Id.* at 821–22.

145. *See* Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases 3 (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

146. *Id.* at 3.

147. *See* Alison Noon, *FBI Director Vows to Treat Hacked Companies As 'Victims'*, LAW360 (Mar. 7, 2018), https://www.law360.com/articles/1019414.

along to federal regulators.[148] The FBI's assurances appear to be motivated by its desire to be alerted by companies of cybersecurity incidents as soon as possible.[149] Wray also suggested that waiting to involve the authorities following a data breach may make a company appear more culpable to what Wray described as "less-enlightened enforcement agencies."[150]

Numerous other costs associated with data breaches, but outside the scope of this article, must be considered and addressed in order to ensure comprehensive coverage for a company's losses.[151] The above discussion demonstrates some of the fallout that can arise specifically due to the theft or accidental disclosure of private information belonging to third parties.

## III. INSURING AGAINST THE RISKS ASSOCIATED WITH PRIVACY CLAIMS

As illustrated in the previous Part, there are myriad risks confronting companies relating to privacy claims that are asserted following a cybersecurity event.[152] As with most risk, prudent businesses should seek, and in some cases may be required,[153] to hedge against those risks through insurance coverage. These risks, however, are relatively new and are rapidly developing as a result of new technology and responsive legislation that has given rise to new liabilities.[154] These developments have made potential damages extremely difficult to predict. Because the policies underwriting these risks are similarly new and developing, it can be difficult for companies to know what type of coverage they should employ to cover their bases. Furthermore, given the novelty and the small sample size of incidents that can be studied,

148. *Id.*

149. *See id.* ("[T]here's no way the FBI can continue to navigate the digital environment alone.").

150. *Id.*

151. For example, a company's contracts with vendors and others in the supply chain may trigger payment of contractual penalties if a data breach occurs. *See* Schnuck Mkts., Inc. v. First Data Merch. Servs. Corp., 852 F.3d 732, 734 (8th Cir. 2017); SELCO Cmty. Credit Union v. Noodles & Co., 267 F. Supp. 3d 1292, 1293 (D. Colo. 2017); P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *6 (D. Ariz. May 31, 2016); Buchanan & Gallozzi, *supra* note 130.

152. *See generally supra* Part II.

153. *See* Sean Harrington, *Cyber Insurance: What Minnesota Lawyers Need to Know*, BENCH & B. MINN., Nov. 2015, at 16, 17 (suggesting that businesses may soon "be required by contract with their customers (such as financial institutions) to have cyber insurance").

154. *See supra* Section II.A.2 (discussing statutory privacy claims); *supra* Section II.B (describing government and regulatory investigations).

insurers are still developing the approach and appetite for the market for cyber insurance.

Nonetheless, the demand for cyber-related insurance coverage is growing.[155] More and more companies are choosing, whether of their own volition or at the behest of their lenders, customers, or other constituents, to obtain coverage relating to certain cyber risks.[156] This growing market is providing insurers with greater clarity and confidence in insuring against cyber risks. However, a number of questions remain open, and policyholders still have an array of options to consider in determining what type of coverage will best fit their needs. While Commercial General Liability (CGL) and other legacy insurance policies, that is, familiar policies which have been in use for many years, traditionally are in large part based on standard forms that employ similar language across providers, there is not, of yet, standardized wording for cyber policies. A company's solid awareness of its cyber risk, including the need to protect against the privacy claims described above, is essential to forming an idea of what type of coverage is required.

This Part will examine the types of coverage that are available to companies seeking to protect against the risks described in the second Part. This includes an overview of how each type of coverage might protect against certain risks, an analysis of the issues that have been addressed by the courts with regard to the application of certain coverages to specific cyber breaches for which companies have sought coverage, and a review of other issues of which businesses should be aware when assessing how to most effectively use insurance to mitigate certain cyber risks.[157]

### *A. Commercial General Liability Coverage*

For a number of years, companies have primarily relied on their CGL coverage to recoup their damages from cyber risks.[158] The

155. See Dan Twersky, Andrew Ko & Judy Xiang, *Brace Yourselves: Global Cyberinsurance Demand Is Coming*, WILLIS TOWERS WATSON (July 26, 2017), https://www.willistowerswatson.com/en/insights/2017/07/decode-cyber-brief-global-cyberinsurance-demand-is-coming (suggesting that demand for cyber insurance is rising, particularly in the United States, in response to increased privacy legislation and strict data breach notification statutes).

156. *Cyber Insurance Premium Volume Grew 35% to $1.3 Billion in 2016*, INS. J. (June 23, 2017), https://www.insurancejournal.com/news/national/2017/06/23/455508.htm.

157. *See generally infra* Sections III.A–.C.

158. *See* Jay Shelton, *FYI: Cyber Claims Excluded from General Liability Coverage*, ASSURANCE (Nov. 20, 2014), https://www.assuranceagency.com/blog-post/fyi-cyber-claims-excluded-from-general-liability-coverage.

emerging trend is for businesses to employ new cyber policies, in addition to their CGL policies, to specifically address cyber-related threats. Nonetheless, it is still important to understand how certain cyber issues will be handled under standard CGL policies. Also, because these legacy policies are the most prevalent forms of coverage, there has been the most significant development of case law interpreting the application of these policies to different cyber-related events.[159]

1. Coverage B

As discussed herein, much of the litigation of cyber issues relating to CGL policies has arisen relating to the application of Coverage B. Standard Coverage B policies provide coverage for personal and advertising injuries, including, potentially, the privacy claims discussed *supra* in Part II.[160] Language in the standard Insurance Services Office (ISO) form provides that such coverage may be available following "oral or written publication, in any manner, of material that violates a person's right of privacy."[161] Whether a cyber issue constitutes a violation of a person's right of privacy could depend on the specifics of the breach. Therefore, the analyses performed by various courts in handling this issue have necessarily been very fact specific and, as a result, have generated conflicting results regarding whether Coverage B will apply in the wake of a data breach.[162] One of the main questions that has arisen for courts in evaluating whether coverage B applies to a data breach, as discussed *infra*, is whether the breach constituted a "publication."[163] In considering this question, courts have looked at how information was disseminated and who was responsible for the spread or loss of

159. Indeed, in one of the only cases dealing directly with a cyber policy, P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *8 (D. Ariz. May 31, 2016), which is discussed at greater length *infra*, the court "turned to cases analyzing commercial general liability insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same." *P.F. Chang's*, 2016 WL 3055111, at *8.

160. *See* Craig F. Stanovich, *No Harm, No Coverage—Personal and Advertising Injury Liability Coverage in the CGL (Part 1)*, INT'L RISK MGMT. INST., INC. (Jan. 2007), https://www.irmi.com/articles/expert-commentary/no-harm-no-coverage-personal-and-advertising-injury-liability-coverage-in-the-cgl-(part-1).

161. *See* ISO PROPERTIES, INC., COMMERCIAL GENERAL LIABILITY COVERAGE FORM CG 00 01 12 07, at 14 (2006), http://www.tmsic.com/pdfs/CommercialGeneral LiabilityCoverageForm_OccurrenceBasis.pdf; *see also* Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 957 F. Supp. 2d 1135, 1140 (C.D. Cal. 2013), *aff'd*, 635 F. App'x 351 (9th Cir. 2015).

162. *See* Cynthia Larose, *On the 12th Day of Privacy, ISO gave to me. . .*, MINTZLEVIN (Dec. 24, 2013), https://www.privacyandsecuritymatters.com/2013/12/on-the-12th-day-of-privacy-iso-gave-to-me/.

163. *See, e.g.*, Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014).

information.[164] We set forth below how some courts have treated cyber-related insurance issues under traditional policies.[165]

a. *Big 5 Sporting Goods Corp. v. Zurich American Insurance Co.*

In *Big 5 Sporting Goods Corporation v. Zurich American Insurance Co.*,[166] the Ninth Circuit affirmed the district court's ruling and concluded that because all of the underlying claims arose from the "alleged violation of the statutory right to privacy," coverage was barred by the applicable policies' statutory violations exclusions, and the carriers had no duty to defend.[167]

*Big 5* involved two different carriers with similar general liability policy exclusions.[168] The court described the first policy as barring "coverage for personal and advertising injury arising directly or indirectly out of any action or omission that violates or is alleged to violate any statute."[169] The second policy barred coverage, as summarized by the court, for "personal and advertising injury arising out of the violation of a person's right of privacy created by any state or federal act," and also contained a second exclusion barring coverage for "personal and advertising injury arising directly or indirectly out of any action or omission that violates or is alleged to violate any statute that prohibits or limits the sending, transmitting, communicating, or distribution of material or information."[170] The district court concluded that these provisions barred coverage for statutory violations, "as well as any act or omission that [arose] directly or indirectly from an alleged violation" of a statute.[171] The Ninth Circuit affirmed that ruling.[172]

The underlying claims alleged so-called "ZIPcode violations" of the Song-Beverly Consumer Warranty Act,[173] a California state law, which created a statutory right of privacy.[174] Among other things, the Song-Beverly Act prohibits entities that accept credit cards in business

164. *See id.*
165. *See infra* Sections III.A.1.a–.c.
166. Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 635 F. App'x 351 (9th Cir. 2015).
167. *Id.* at 353.
168. *See id.*
169. *Id.* (emphasis omitted).
170. *Id.*
171. *Id.* (emphasis omitted).
172. *See id.*
173. Song-Beverly Consumer Warranty Act, CAL. CIV. CODE §§ 1790–1795.8 (West 2018).
174. Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 957 F. Supp. 2d 1135, 1137 (C.D. Cal. 2013), *aff'd*, 635 F. App'x 351 (9th Cir. 2015).

transactions from requiring a cardholder to write or provide personal identification information, such as zip codes, on the transaction form.[175] The insured affirmed that in addition to facing statutory violations, it was forced to defend common law and California constitutional right to privacy claims that were separate from the violations of the Song-Beverly Act.[176] The Ninth Circuit rejected this argument, finding instead that California law "does not recognize any common law or constitutional privacy right causes of action for requesting, sending, transmitting, communicating, distributing, or commercially using any ZIP Codes."[177] The court found that "[t]he only possible claim [was] for statutory penalties, not [common law] damages."[178] Thus, the Ninth Circuit determined that the right to privacy claims against the insured did not entitle the insured to a defense because they were not viable as a matter of law and constituted improper "boilerplate pleading."[179] The Ninth Circuit agreed with the district court that because all of the underlying claims arose from violations of the Song-Beverly Act, the carriers had established as a matter of law that there was no conceivable theory under which the claims in the underlying actions warranted coverage.[180]

Although no two policies are identical, *Big 5* teaches that companies shopping for coverage relating to privacy claims should ensure that the policy does not exclude coverage for statutory violations. A policy that does exclude such coverage should only permit the insurer to deny coverage where a statutory violation is proven, and not merely pled. This advice is particularly imperative in view of the multiple statutory causes of action that are available to plaintiffs following a data breach.[181]

b. *Innovak International, Inc. v. Hanover Insurance Co.*

In *Innovak International, Inc. v. Hanover Insurance Co.*,[182] the insured brought an action against its insurance provider, Hanover Insurance Company ("Hanover"), claiming that Hanover was required to defend it in numerous suits that had arisen following a data breach that compromised users' personal private information (PPI).[183] Innovak

175. *See* CAL. CIV. CODE §§ 1790–1795.8.
176. *Big 5 Sporting Goods*, 635 F. App'x at 353–54.
177. *Id.* at 354.
178. *Id.*
179. *See id.* (quoting Swain v. Cal. Cas. Ins. Co., 99 Cal. App. 4th 1, 8–9 (2002)).
180. *See id.*
181. *See, e.g.*, *supra* Section II.A.1.b (discussing negligence claims arising from violation of statute); *supra* Section II.A.2 (surveying selected statutory privacy claims).
182. Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340 (M.D. Fla. 2017).
183. *Id.* at 1341–42.

International Inc. ("Innovak") was a provider of "payroll computer software [used in] schools, school districts, and . . . other entities [throughout] the United States."[184] The company "was subject [to] a data breach when hackers appropriated" the PPI that the company had stored and made accessible through the company's Internet portal.[185]

Innovak sought coverage under Coverage B, arguing that Hanover had a duty to defend the underlying action because the plaintiffs "plainly and unequivocally allege that Innovak negligently prepared, designed and published software that allowed private personal information to be known by third parties."[186] Innovak asserted "that Coverage B provides . . . coverage for claims alleging any publication of material that violates a person's right to privacy, whether the publication is directly or indirectly committed by the insured."[187]

Hanover moved for summary judgment on the ground that Coverage B was inapplicable because the plaintiffs alleged appropriation, and not publication, of their PPI by third parties.[188] Even if the plaintiffs had alleged publication, the insurer asserted that Coverage B would apply only to intentional acts by the insured, not to acts by third-party hackers.[189] Hanover also argued that if the court construed plaintiffs' claims as alleging publication by Innovak, Coverage B still would not be triggered because it applies only to intentional acts of an insured, and the underlying claims alleged only that Innovak was negligent.[190]

Ultimately, the court determined that there was no coverage because the underlying allegations failed to allege publication by Innovak.[191] Rather, as the court pointed out, the hackers perpetrated the alleged publication.[192] Further, the court observed that:

> Innovak materially mischaracterizes the allegations of the Underlying Complaint. Nowhere in the Underlying Complaint do the Underlying Claimants contend that their PPI was "published," whether by third party hackers or by Innovak. However, even if the Court views the alleged data breach as an alleged publication of the Underlying Claimants' PPI, the Underlying Claimants do not allege that Innovak published their information. Innovak apparently concedes the point as it contends that the Underlying Claimants' allege that Innovak "published

184. *Id.* at 1342.
185. *Id.*
186. *Id.* at 1344.
187. *Id.*
188. *Id.*
189. *Id.*
190. *Id.*
191. *Id.* at 1347.
192. *Innovak Int'l*, 280 F. Supp. 3d at 1348.

> software," rather than the Underlying Claimants' private information. However, publication of Innovak's software does not "violate[] [the Underlying Claimants'] right of privacy" as required for coverage under Coverage B. The act that violates the claimants' right of privacy is the publication of their PPI, and the Underlying Claimants have not alleged that Innovak directly or indirectly committed that act. Innovak makes several arguments to the contrary, but the Court finds each argument unavailing.[193]

The publication issue addressed in *Innovak* is one of the major shortcomings of CGL policies as they apply to cyber-related threats. Companies seeking to insure against such contingencies should be aware that courts will not only consider *whether* a publication occurred but may also consider *by whom* the publication was perpetrated. Because the language of the policy at issue will control, companies can increase the scope of coverage by demanding policy language that covers privacy claims irrespective of who makes the information public.

c. *Zurich American Insurance Co. v. Sony Corp. of America*

In *Zurich American Insurance Co. v. Sony Corp. of America*,[194] a New York state trial court determined in a bench ruling that an insurer was not required to provide coverage to its insured as a result of a data breach that Sony had experienced when third-party hackers had pilfered the personal information of tens of millions of users resulting in losses estimated as high as $2 billion.[195] Sony Corporation of America ("Sony") sought indemnification from Zurich American Insurance Company ("Zurich") under Coverage B of its CGL policy.[196] The court, however, denied coverage on the basis that the data breach had not resulted in a "publication" for purposes of coverage B.[197]

The court did find that publication had occurred.[198] Indeed, it stated that "by just merely opening up that safeguard or that safe box where all of the information was . . . my finding is that that is publication."[199]

193. *Id.* at 1347 (alteration in original) (citation omitted).

194. Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014).

195. *See id.* at *67–72; *see also* Young Ha, *N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation*, INS. J. (Mar. 17, 2014), http://www.insurancejournal.com/news/east/2014/03/17/323551.htm.

196. *See* Sony Defendants' Answer to Second Amended Complaint, Counter-Claims, and Cross-claims, for Declaratory Judgment and Damages Due to Breach of Contract and Bad Faith at 19–20, 22–23, *Zurich*, 2014 N.Y. Misc. LEXIS 5141 (No. 651982/2011); Ha, *supra* note 195.

197. *Zurich*, 2014 N.Y. Misc. LEXIS 5141, at *69.

198. *Id.*

199. *Id.*

However, the court ultimately concluded that coverage must be denied because the publication had not been perpetrated by Sony.[200] As the judge noted, "[t]his is a case where Sony tried or continued to maintain security for this information. It was to no avail. Hackers . . . criminally got in. They opened it up and they took the information."[201]

Because the act of publication was perpetrated by the hackers, rather than by Sony, the court found that it was not covered under the policy.[202] The court stated that "[the policy] requires the policyholder to perpetrate or commit the act. . . . It cannot be expanded to include [third-]party acts."[203] It further explained that the language of the policy in paragraph E (dealing with "oral or written publication in any manner of material that violates a person's right of privacy") specifically required "some kind of act or conduct by the policyholder in order for coverage to be present."[204] The judge, however, found "that there was no act or conduct perpetrated by Sony, but it was done by [third-]party hackers illegally breaking into that security system. And that alone does not fall under paragraph E's coverage provision."[205]

Some questioned the trial court's ruling in *Zurich* and the case was immediately appealed.[206] The case was litigated through oral argument, but was ultimately settled out of court prior to resolution of the appeal, leading some to speculate that Zurich was more comfortable living with the payment than with the potential bad precedent should the decision be overturned.[207] As with *Innovak*, *Zurich* suggests that companies would do well to ensure that privacy claims based on publication will be covered by their suite of insurance policies irrespective of whether the insured or a third party actually effectuates the publication.

2. Access

Another issue of which potential insureds should be aware and of which courts have taken notice focuses on whether it is necessary that a third party actually "access" the information in question. As illustrated in

200. *Id.*
201. *Id.*
202. *See id.* at *70.
203. *Id.*
204. *Id.* at *72.
205. *Id.*
206. *Cf.* Joan M. Cotkin & James H. Vorhis, *Insurers Pay to Avoid a Precedent Finding CGL Coverage for a Cyberbreach—the* Zurich v. Sony *Settlement*, LEXOLOGY (Apr. 30, 2015), https://www.lexology.com/library/detail.aspx?g=e93e0eb9-b27e-4b44-8d0f-d9a50b5d5e25; Jeff Sistrunk, *Sony, Zurich Settle Data Breach Coverage Battle*, LAW 360 (Apr. 30, 2015), https://www.law360.com/articles/650046/sony-zurich-settle-data-breach-coverage-battle.
207. *See* Cotkin & Vorhis, *supra* note 206; Sistrunk, *supra* note 206.

the cases below, courts have taken somewhat divergent stances in this regard.[208]

a. *Recall Total Information Management, Inc. v. Federal Insurance Co.*

In *Recall Total Information Management, Inc. v. Federal Insurance Co.*,[209] the plaintiff, Recall Total Information Management, Inc. ("Recall Total"), had contracted with IBM to transport and store certain electronic media and records of IBM which contained personal information of hundreds of thousands of current and former IBM employees.[210] Recall Total subcontracted the actual transportation services to a company called Executive Logistics ("Ex Log").[211] On one occasion, a cart holding IBM tapes that contained electronic personal information fell from one of Ex Log's vehicles during transport, and, before the cart could be retrieved, 130 tapes had been removed and were never recovered.[212]

Despite the fact that there was no indication that someone was misappropriating the personal information contained in the lost files, IBM took immediate and significant steps, to the tune of $6 million, to mitigate potential damages that might arise from the breach, including setting up a call center and providing one year of credit monitoring to all those affected.[213] IBM consequently sought recovery of those mitigation costs from Recall Total and from Ex Log.[214] Recall Total, which was named as an additional insured on Ex Log's policy, in turn sought coverage pursuant to Ex Log's CGL policy held with Federal Insurance Company.[215]

The trial court determined that Ex Log's insurance policy with Federal Insurance Company, covering personal injury for invasion of privacy, did not cover the data breach in question because, although IBM had incurred substantial expense addressing the data loss, this could not satisfy the "personal injury" requirement of its policy.[216] This was because IBM, as a corporation, was not a person for purposes of invasion of privacy law and "there [was] no allegation that its right to privacy was violated."[217] Furthermore, in the absence of any proof that anyone whose

208. *See infra* Sections III.A.2.a–.b.
209. Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664 (Conn. App. Ct. 2014), *aff'd*, 115 A.3d 458 (Conn. 2015).
210. *Id.* at 667.
211. *Id.*
212. *Id.*
213. *See id.* at 668.
214. *Id.*
215. *See id.* at 667–68.
216. *See id.* at 668.
217. *Id.*

personal information was lost had suffered identity theft or any other privacy violation in the four years since the loss of the data, the trial court granted the defendant insurers' motion for summary judgment.[218]

The appellate court affirmed the lower court's decision and reiterated that "the dispositive issue is not loss of the physical tapes themselves; rather, it is whether the information in them has been *published*."[219] The court noted that "[t]he plaintiffs contend[ed] that the mere loss of the tapes constitute[d] a publication, and has [sic] alleged that the information was *published* to a thief."[220] The court explained that publication is not simply making information available, but rather it is *communicating* the information that is paramount.[221] Further, the court specified that it "believe[d] that *access* is a necessary prerequisite to the communication or disclosure of personal information."[222] Because IBM could not show that anyone had accessed the personal information that was stored on the tapes, IBM therefore could not show publication and, thus, was not entitled to coverage under the policy.[223]

b. *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, L.L.C.*

In contrast to *Recall Total*, in *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, L.L.C.*[224] the court found personal information to have been sufficiently *published* for coverage purposes, even where there was no allegation that the public information had been accessed by any unauthorized user.[225] The underlying litigation in *Portal* arose after Portal Healthcare Solutions, L.L.C. ("Portal"), which "specializ[es] in the electronic safekeeping of medical records for hospitals, clinics, and other medical providers," allegedly failed to safeguard certain confidential medical information that had been provided to it and allowed that information to be posted publicly on the Internet.[226]

Portal was insured under two substantially similar policies it had procured from Travelers Indemnity Company of America ("Travelers"), and Portal sought to require Travelers to defend the underlying

218. *See id.* at 668–69.
219. *Recall Total*, 83 A.3d at 672.
220. *Id.*
221. *See id.*
222. *Id.* (emphasis added).
223. *See id.* at 673.
224. Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C., 35 F. Supp. 3d 765 (E.D. Va. 2014), *aff'd*, 644 F. App'x 245 (4th Cir. 2016).
225. *See id.* at 770–71.
226. *See id.* at 767–68.

litigation.[227] In relevant part, those policies provided that Travelers was obligated to defend Portal for "'publication' giving 'unreasonable publicity' to, or 'disclos[ing]' information about, a person's private life."[228] The district court determined that Travelers was bound to defend Portal in the underlying action because "exposing material to . . . online searching . . . does constitute a 'publication' of electronic material" and, therefore, was covered by the policy.[229] The court further explained that because the medical records had "at least 'potentially or arguably'" been placed before the public, they had been published for coverage purposes.[230] The Fourth Circuit affirmed the lower court's decision.[231]

The above cases further illustrate the need for broad policy language relating to privacy claims following a data breach. Ideally, coverage should apply irrespective of (1) who permitted unauthorized access to the data; and (2) whether the data was actually accessed impermissibly versus simply being made available for unauthorized access by a third party.

3. Coverage A

Other cyber-related litigation has involved requests for coverage pursuant to Coverage A, which covers bodily injury and property damage.[232] However, some writers have suggested that coverage may be available for cyber harms under Coverage A as a "bodily injury" in a situation where "victims of a cyber event[,] such as a data breach[] where personal[,] financial, and identifying information has been breached and used to perpetrate identity theft," suffer emotional distress as a result of the cyber event.[233] Notably, in *Innovak*, the underlying claimants' allegations included that "as a result of Innovak's conduct, they suffered, [among other things], 'psychic injuries,' including 'stress, nuisance, loss of sleep, worry, and the annoyance of having to deal with issues resulting from the Innovak data breach.'"[234] However, as the court noted, Innovak did not seek coverage under Coverage A in the action, and, therefore, the

227. *See id.*
228. *Id.* at 769 (alteration in original).
229. *Id.* at 770.
230. *Id.*
231. Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C., 644 F. App'x 245, 248 (4th Cir. 2016).
232. *See* Meghan E. Ruesch, *Show Me the Bitcoin! The Costs of Cyber Risks and the Cyber-Insurance Coverage Landscape*, 12 IN-HOUSE DEF. Q. 66, 69 (2017).
233. *Id.* (citing TL Sharp et al., *Exploring the Psychological and Somatic Impact of Identity Theft*, 49 J. FORENSIC SCI. 131 (2004)).
234. Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1342 (M.D. Fla. 2017).

court did not consider whether such coverage would apply based on the underlying allegations.[235]

Cases addressing whether certain cyber breaches may result in coverage pursuant to a CGL policy as "property damage" have produced divergent results.[236] Under the standard CGL policy, the term "property damage" encompasses "'physical injury' or 'loss of use' of 'tangible property.'"[237] However, "whether 'data' qualifies as 'tangible property'" has been treated differently in different courts, with "[t]he majority of cases addressing this issue having found that 'data' does not constitute 'tangible property' capable of sustaining damage."[238] On the other hand, courts that have found that data can be considered tangible property have looked to the hardware on which the data is stored.[239]

Policy providers have made efforts to limit the scope of CGL policies, and "specifically [have] exclude[d] 'electronic data' from 'tangible property' under the definition of 'property damage.'"[240] Indeed, the standard CGL ISO form now "excludes damages 'arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.'"[241] Where insurers have expanded exclusions and limitations to "property damage" coverage, they will argue that the policies "indicate[] a clear intent . . . not to cover data breaches under traditional [c]overage."[242]

Despite the fact that courts will, in general, broadly interpret coverage language, the cases discussed herein demonstrate that a number of courts have been reluctant to apply general CGL language, whether Coverage A, B, or otherwise, to cyber-related issues. Additionally, while many CGL policies may continue to cover various aspects of cyber breaches, the trend is for insurers to write cyber coverage out of the general policies in favor of more specific plans.[243] Indeed, in 2014, the ISO standard CGL policy added an exclusion which eliminates coverage

235. *See id.* at 1344.

236. *Compare* Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003) (finding that data does not constitute tangible property for purposes of Coverage A coverage), *with* London-Sire Records, Inc. v. Doe, 542 F. Supp. 2d 153, 171 (D. Mass. 2008) (determining that data that was stored on a hard disk was tangible property for coverage purposes).

237. Ruesch, *supra* note 232, at 69.

238. *Id.* (citing *Am. Online*, 347 F.3d at 89).

239. *Id.* (citing NMS Servs. Inc. v. Hartford, 62 F. App'x 511 (4th Cir. 2002); Capitol Records, LLC v. ReDigi, Inc., 934 F. Supp. 2d 640 (S.D.N.Y. 2013); *London-Sire Records*, 542 F. Supp. 2d at 153).

240. *Id.*

241. *Id.*

242. *Id.*

243. *See id.* at 69–70 (explaining that many insurers have begun implementing mechanisms to limit the scope of cyber-related coverage in CGL policies).

in CGL polices that is "for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."[244]

### *B. Cyber Policies*

As a result of increasing cyber risks and decreasing availability of coverage under recent CGL policies, heightened demand has increased for policies that are created specifically to address cyber threats. The market for cyber risk insurance policies has been growing rapidly, with total premiums, by some estimates, reaching approximately $4 billion in 2017, which is almost a 25 percent increase from the previous year's estimated $3.25 billion in premiums.[245] While the market for cyber-related policies is growing, with approximately 70 insurers now offering cyber-related policies, still only roughly 15 percent of insureds have opted for a policy specifically designed to cover cyber threats.[246] This rapid development in the market has enticed insurance companies to develop a wide array of products in response to the various cyber-related issues that companies may face.[247] In general, insurers have been developing cyber insurance policies that fall into a wide variety of categories including the following: Liability; Network Security Liability; Privacy Liability; Media Liability; Remediation/Breach Response Costs; Regulatory Fines and/or Penalties; Cyber Extortion; Fund Transfers Fraud; Business Interruption; Data Recovery/Restoration; and PCI (Payment Card Industry) Credit Card Fines and Penalties.[248]

These types of policies provide coverage that can generally be separated into three basic categories:

- Liability—[which includes] defense and settlement costs for the liability of the insured arising out of its failure to properly care for private data[;]

244. *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INS. J. (July 18, 2014), https://www.insurancejournal.com/news/east/2014/07/18/332655.htm.

245. RICHARD S. BETTERLEY, THE BETTERLEY REPORT, CYBER/PRIVACY INSURANCE MARKET SURVEY—2017, at 6 (2017), https://www.irmi.com/docs/default-source/authoritative-reports/betterley-executive-summaries/cyber-privacy-media-liability-summary-2017.pdf?sfvrsn=6.

246. *See* AON INPOINT, GLOBAL CYBER MARKET OVERVIEW: UNCOVERING THE HIDDEN OPPORTUNITIES 4 (2017), http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf.

247. *See id.*

248. Ruesch, *supra* note 232, at 70 (citing RICHARD S. BETTERLEY, THE BETTERLEY REPORT: CYBER/PRIVACY INSURANCE MARKET SURVEY—2016 (2016)).

- Remediation—[which serves to cover] response costs following a data breach, including investigation, public relations, customer notification, and credit monitoring[; and]
- [Fines and/or Penalties, which includes both:]
    - Regulatory Fines and/or Penalties—[which cover] the costs to investigate, defend, and settle fines and penalties that may be assessed by a regulator . . . [, and]
    - PCI (Credit Card) Fines and Penalties—[which typically] include[] forensic services and card reissuance costs[.][249]

In addition to understanding what can be covered, companies in the market for cyber insurance should be informed as to what may trigger coverage and what type of data will be covered.

While the number of cyber policies available is growing, in turn providing businesses with better clarity and understanding as to what coverage they are actually purchasing, there remain a number of risks and unknowns of which policyholders should be aware. For one, the case law surrounding cyber-specific policies is relatively sparse. Indeed, only two cases have litigated the application of the terms of a cyber policy.[250] The first case, which involved Cottage Health System, was dismissed without prejudice to allow the parties to pursue mediation—although notably the case has since been refiled in California state court and is currently pending—and the second case, which involved P.F. Chang's China Bistro, Inc. ("P.F. Chang's"), was decided by a court that issued an unpublished opinion.[251] As was the case in *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*,[252] courts considering how insurance law applies to cyber policies may look to how such coverage

249. BETTERLEY, *supra* note 245, at 9.

250. *See* P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1 (D. Ariz. May 31, 2016); Columbia Cas. Co. v. Cottage Health Sys., No. 2:15-cv-03432, 2015 WL 4497730, at *2 (C.D. Cal. July 17, 2015) [hereinafter *Cottage Health I*]; Cottage Health Sys. v. Columbia Cas. Co., No. 16CV02310 (Cal. App. Dep't Super. Ct. filed May 31, 2016) [hereinafter *Cottage Health II*].

251. *See* P.F. Chang's, 2016 WL 3055111, at *1; *Cottage Health I*, 2015 WL 4497730, at *2; *Cottage Health II*, No. 16CV02310. The main issue in *Cottage Health* involves whether the insureds coverage following a data breach should be excluded based on human error in failing "to continuously implement the procedures and risk controls identified in the Insured's application." *See* Buchanan & Gallozzi, *supra* note 130. This litigation is currently pending in separate actions that have been filed in both state court and federal court, although the federal action has been stayed pending the state court's determination. *See Cottage Health I*, 2015 WL 4497730, at *2; *Cottage Health II*, No. 16CV02310.

252. P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1 (D. Ariz. May 31, 2016).

has been treated under other general policies such as CGL policies in making their determinations.[253] For example, exclusions in cyber policies are numerous and varied, as in other insurance policies, and must be taken into careful consideration when interpreting a policy. Indeed, the court's application of the insurance provider's exclusion to deny coverage in the *P.F. Chang's* case is a notable recent development dealing specifically with a cyber-specific insurance policy.[254]

In *P.F. Chang's*, Federal Insurance Company ("Federal") sold a cyber risk insurance policy to P.F. Chang's parent company, Wok Holdco LLC, that covered P.F. Chang's for "direct loss, legal liability, and consequential loss resulting from cyber security breaches."[255] The policy was advertised as being "flexible" and "designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world."[256] After P.F. Chang's was the victim of a cyber breach wherein approximately 60,000 credit card numbers belonging to its customers were stolen, P.F. Chang's sought coverage from Federal from which it bought a Chubb cyber policy.[257] The Chubb cyber policy covered the insured as well as provided third-party coverage.[258] Federal paid approximately $1.7 million defending the class action case and orchestrating a forensic investigation.[259] However, Federal denied coverage relating to certain MasterCard assessments, totaling approximately $1.9 million, that MasterCard had charged to Bank of America Merchant Services ("BAMS"), P.F. Chang's credit card processor, for the costs of replacement cards, notifications to consumers, and reimbursement for fraudulent charges.[260] P.F. Chang's entered into an agreement with BAMS to assume liability for such assessments as part of their processing agreement; however, Federal claimed that because P.F. Chang's agreed to the assessment by contract, the insured was not entitled to coverage under their cyber policy.[261]

The Federal policy insured "[e]xtra [e]xpenses an [i]nsured incurs during the [p]eriod of [r]ecovery [s]ervices due to the actual or potential impairment or denial of [o]perations resulting directly from [f]raudulent

253. *Id.* at *8 (explaining that cases that examine CGL policies serve as an appropriate guide for the court in deciding cases involving cyber-related issues "because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same").

254. *See infra* notes 264–68 and accompanying text.

255. *P.F. Chang's*, 2016 WL 3055111, at *1.

256. *Id.*

257. *Id.* at *2.

258. *Id.* at *4.

259. *Id.* at *2.

260. *See id.*

261. *Id.* at *5.

[a]ccess or [t]ransmission."[262] P.F. Chang's argued that all of MasterCard's charges fell into the categories covered under the policy.[263]

The court, however, determined that the policy unequivocally barred coverage for "any [l]oss on account of any [c]laim, or for any [e]xpense . . . based upon, arising from or in consequence of any . . . liability assumed by any [i]nsured under any contract or agreement."[264] P.F. Chang's, therefore, was unable to rely upon its Coverage B coverage because it had assumed BAMS's liability as part of their processing agreement.[265]

In its analysis, the court "turned to cases analyzing [CGL] insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same."[266] The court relied on the fact that cases interpreting CGL policies generally conclude that liability exclusions also apply to "the assumption of another's liability, such as an agreement to indemnify or hold another harmless."[267] Although P.F. Chang's sought to persuade the court that the exclusion did not apply in cases where the insured had a responsibility to a third party even if it had not assumed liability, the court found that P.F. Chang's had failed to demonstrate that it "would have been liable for [MasterCard's] [a]ssessments absent its agreement with BAMS."[268]

While the *P.F. Chang's* decision involved liability predicated on contract rather than harm to a third party resulting from a common law or statutory privacy claim, the decision illustrates how a court might analyze a coverage dispute involving a cyber policy.

### *C. Other Policies*

Companies seeking to protect themselves from cyber threats may find additional protection against at least certain aspects of these risks through various insurance policies other than standard CGL or cyber-specific policies. To name a few, coverage for cyber breaches may be available from insurers through crime policies, errors and omissions policies, and director and officer policies.[269] However, it is still critical

262. *Id.* at *6 (emphasis omitted).
263. *See id.* at *4.
264. *Id.* at *7
265. *P.F. Chang's*, 2016 WL 3055111, at *7–8.
266. *Id.* at *8.
267. *Id.* (quoting Desert Mountain Props. Ltd. P'ship v. Liberty Mut. Fire Ins. Co., 236 P.3d 421, 432 (Ariz. Ct. App. 2010)).
268. *Id.*
269. *See* Karin S. Aldama & Tred R. Eyerly, CYBER POLICIES—THE NEXT WAVE 4 (2018), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2018-insurance/written-materials/cyber-policies.authcheckdam.pdf. To the extent that any of these policies exclude coverage for the wrongful or intentional conduct of

that businesses understand that while policies such as these may cover various aspects of cyber issues, it is very likely that they will not cover all possible losses. Therefore, it is imperative that businesses be aware of the extent to which these types of policies may actually provide coverage following a cyber event.

For example, cyber breaches are generally also crimes.[270] If hackers appropriate information by illegally accessing the network of a given company, their obtaining of the information is likely a crime, but that does not necessarily mean it will be covered by a company's crime policy. This may be the case when the negligent acts of a company, albeit indirectly, allow for a cyber-related crime to be perpetrated.

Consider *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*,[271] in which Principle Solutions Group, LLC ("Principle") was the victim of a fraudulent scheme involving the use of email.[272] Principle's controller received a request to approve a wire-transfer that purportedly came from one of Principle's managing directors.[273] The request was, in actuality, fraudulent, and the controller, despite performing a series of steps in an attempt to verify the authenticity of the request, ultimately approved the transfer.[274] By the time the company realized that the email requests received by the controller were indeed fraudulent, it was too late to recover the approximately $1.7 million transfer.[275] The company thereafter sought to recover the value of the lost funds pursuant to the "Computer and Funds Transfers Fraud" category of their commercial crime policy.[276]

The policy provided coverage for "[l]oss resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit [Principle's] 'transfer account' and transfer, pay or deliver 'money' or 'securities' from that account."[277] The insurer denied coverage on the basis that the transfer in question was not actually effectuated by the criminals but was made legitimately by the controller.[278] The court stated that it was reasonable for Principle's insurer, Ironshore Indemnity, Inc.,

---

directors, officers, or other agents of the insured company, the insured can maximize coverage if the policy language only permits the insurer to deny coverage once such a wrongful act is proven, rather than only pled.

270. *See Cyber Crime*, FBI, https://www.fbi.gov/investigate/cyber (last visited Apr. 26, 2018).

271. Principle Sols. Grp., LLC v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).

272. *Id.* at *1.

273. *Id.*

274. *See id.*

275. *Id.* at *2.

276. *See id.*

277. *Id.*

278. *Id.* at *2, *4.

to interpret the language to "require an immediate link between the injury and its cause."[279] Nonetheless, the court also found plaintiff's interpretation to be reasonable, and in light of the ambiguity, ruled in favor of the insured.[280]

Compare, however, the result in *Principle Solutions* to the result in *Apache Corp. v. Great American Insurance Co.*[281] In *Apache Corp.*, a corporation was again the victim of cyber-related crime that involved the use of email.[282] The criminals posed as a vendor to the company and induced an Apache Corporation ("Apache") employee to change the wiring instructions for the company.[283] As a result, the company wired the equivalent of approximately $7 million to the new (fraudulent) account, approximately $2.4 million of which they were unable to recover.[284]

The company asserted coverage from its insurance provider under the computer fraud provision of its crime-protection insurance policy.[285] The policy language states:

> [The insurer] will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or
>
> b. to a place outside those premises.[286]

The insurance company denied coverage asserting that the "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds."[287] The district court awarded summary judgment to Apache, determining that "the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor.'"[288]

On appeal, the Fifth Circuit vacated the grant of summary judgment to the plaintiff and remanded to the district court.[289] The court

279. *Id.* at *5.
280. *Id.*
281. Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016).
282. *Id.* at 253.
283. *See id.*
284. *Id.* at 253–54.
285. *Id.* at 254.
286. *Id.*
287. *Id.*
288. *Id.* (alteration in original).
289. *Id.* at 259.

determined that it was Apache that changed the account information and initiated the transfers that were sent to the fraudulent account, not the criminals, and, therefore, while "[t]he email was part of the scheme[,] the email was merely incidental to the occurrence of the authorized transfer of money."[290] The court reasoned that interpreting the provision of the policy to cover any fraud where an email was part of the process would convert the policy to one for "general fraud."[291] The court further explained that "viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache elected to pay legitimate invoices," and therefore it "[r]egrettably, . . . sent the payments to the wrong bank account."[292]

As indicated by the divergent outcomes arrived at in these two cases, it is important that companies understand the specifics of the language in their policies. In *Principle Solutions* and *Apache Corp.*, the insureds were seeking coverage for loss that resulted from fraud that was perpetrated through email under categories of policies respectively labeled "Computer and Funds Transfers Fraud" and "Computer Fraud," and yet the specific language of the policies resulted in drastically different results for the affected parties.[293] Therefore, while insureds may want to continue to request the addition of specific cyber provisions to their various non-cyber-specific insurance policies that may fit certain unique needs of the company, it is likely still a best practice for companies to obtain comprehensive cyber-specific policies. As these policies develop, they will likely become more transparent and comprehensible, allowing companies to better understand how its cyber-related issues will be treated by insurers.

## IV. CONCLUSION: SHOPPING FOR AN EFFECTIVE CYBER POLICY RELATING TO PRIVACY CLAIMS

In the cyber events contemplated by this article, criminals infiltrate a company's system in order to profit from the data within that system. Or, just as dangerous, an employee or vendor unwittingly makes the data accessible. The result is that data a company sought to keep secure is breached and, potentially, made available to unauthorized third parties. In these circumstances, companies are at risk of expensive multidistrict or class action litigation in which consumers assert privacy-related claims, including invasion of privacy by publication of private facts,

290. *Id.* at 258.
291. *Apache Corp.*, 662 F. App'x at 258.
292. *Id.* at 259.
293. *See id.* at 253, 258–59; Principle Sols. Grp., LLC v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *2, *5 (N.D. Ga. Aug. 30, 2016).

negligence, and violation of state and federal laws.[294] Moreover, the company may find itself the subject of an investigation brought by the FTC or other government agency.[295] In addition, state law and administrative agency regulations may impose reporting requirements and other obligations on companies who are victims of data breaches.[296]

In the limited judicial interpretations of policies that potentially cover these risks, courts have identified some gaps in coverage.[297] When shopping for insurance policies that will provide comprehensive protection against the risk of privacy-related damages, companies should learn from this guidance and ensure that these gaps are filled by their existing or new policies. The coverage referenced in the examples below refers not only to coverage for losses, but also to the insurer's duty to defend, as these multidistrict or class action claims involve significant litigation expense.

First, an exclusion for statutory violations may create a formidable (and costly) problem for insureds, as the data protection space is increasingly governed by state and regulatory obligations.[298] Accordingly, coverage that excludes statutory violations will be insufficient.

Second, policyholders should ensure that the insurance they purchase provides coverage regardless of whether publication of private information is effectuated by an insured or by a third party (such as hackers or a vendor).[299] Similarly, coverage should exist irrespective of whether the disclosure of third-party data resulted from an affirmative act (such as posting the data on the Internet) or an omission in failing to protect the data (for instance, failing to implement reasonable data security measures).

Third, a comprehensive insurance strategy will also provide coverage even if data is simply lost or stolen and there is no evidence of publication to a third party.[300]

Fourth, coverage should exist even if the damage is only to data or other intangible property.[301]

Fifth, companies should ensure that they are covered for any contractual liability to third parties that might result from a data breach.[302] Because the extent of this risk should be known based upon

294. *See supra* Section II.A.
295. *See supra* Section II.B.
296. *See supra* notes 124–25 and accompanying text.
297. *See supra* Part III.
298. *See supra* Section II.A.2.
299. *See supra* Section III.A.1.
300. *See supra* Section III.A.1.
301. *See supra* Section III.A.2.
302. *See supra* Section III.B.

reference to a company's contracts, companies should ensure that policy limits are high enough to cover any contractual penalties.

Finally, an insured's insurance strategy should address the potential for regulatory investigations, which may otherwise not qualify as litigation giving rise to an insurer's duty to defend.[303] In addition, any reporting obligations or other duties imposed by statute or regulation could result in significant cost for which policyholders may want to purchase coverage.[304]

Although the law in this area of insurance coverage continues to evolve, a company seeking to maximize coverage in the event of a data breach should keep the above suggestions in mind when selecting an insurer.

303. *See supra* Section III.B.
304. *See supra* Section III.B.