INSURANCE FOR CYBER RISKS: A COMPREHENSIVE ANALYSIS OF THE EVOLVING EXPOSURE, TODAY'S LITIGATION, AND TOMORROW'S CHALLENGES

Gregory D. Podolak[*]

[*] Partner and chair of the Cyber Risk practice at Saxe Doernberger & Vita, P.C., a national practice exclusively dedicated to representing policyholders in insurance coverage disputes. I would like to thank Attorneys K. Alexandra Byrd and Michael Barrese, both of SDV, for their diligent efforts and invaluable insight in bringing this article to fruition.

I. INTRODUCTION

Cyber Risk has become the defining risk management discussion of the 21st century, with new and unique exposures surfacing on a seemingly daily basis across all industries. In addition to enhancing security measures, risk managers, general counsel, and Chief Information/Security Officers are actively revisiting their risk transfer and insurance programs to match the growing threat. At the same time, the insurance industry has launched an aggressive campaign, both in the courts and through the modification of policy forms, to avoid covering these types of claims under traditional policies, thus redirecting policyholders into a new, dedicated cyber insurance market.

The risks, and resulting coverage litigation, are evolving exponentially. Because the cyber insurance market is still in its relative infancy, both in terms of underwriting history and key coverage terms and concepts, policyholders would ordinarily expect cyber insurance litigation to develop slowly over the next twenty to thirty years. Many insurers, however, are currently advancing arguments under the guise of avoiding cyber coverage under traditional lines, which could dramatically affect stand-alone coverage. For the reasons discussed in this Article, coverage under traditional lines cannot be completely abandoned and policyholders must actively think forward about how best to position their insurance options in the event of a loss.

Accordingly, Part II explores the current nature of Cyber Risk, including escalating costs, the threat of interconnectivity, and exposure

regardless of industry. Parts III and IV review the diverse, constantly evolving landscape of coverage litigation involving "traditional" insurance policies, with a particular focus on a significant decision[1] currently before the Connecticut Supreme Court—arguably the first of its kind. Part V discusses future developments, analyzing the impact of current litigation under traditional lines on the coverage dialogue under stand-alone policies (the two are more closely related than one might think), and concludes that the current debate over the scope of Cyber Risk coverage will not subside with the emergence of dedicated lines, as policyholders and insurers alike struggle to adequately define the risk and tailor the coverage accordingly.

II. THE SURGE IN CYBER RISK

Despite dominating headlines, the so-called "Cyber Risk" exposure remains vaguely defined for many policyholders. This is not unexpected, as Cyber Risk is inextricably linked to the evolution of technology, and is therefore in a constant state of evolution. Moreover, Cyber Risk is an exposure that transcends industries, and thus forces itself upon policyholders who traditionally have had minimal exposure to technology. As of today, Cyber Risk "generally includes any loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality."[2] As the "most prevalent, widely publicized, and expensive exposure today," the data breach is Cyber Risk's poster child, as Sony, Target, Home Depot, JP Morgan Chase, and most recently, Anthem, have become painfully aware.[3] "In the case of individuals, a data breach involves stolen 'personally identifiable information'" (PII), like credit card information or social security numbers, or "'personal health information'" (PHI), such as medical records.[4] For corporations, a data breach "can involve various forms of sensitive or confidential information, such as client records, bid

[1] Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., No. X07CV095031734S, 2012 WL 469988, at *6 (Conn. Super. Ct. Jan. 17, 2012), *aff'd*, 147 Conn. App. 450 (2014), *cert. granted*, 311 Conn. 925 (2014).

[2] Gregory D. Podolak, *Cyber Risk Coverage Litigation Heats Up as Exposure and the Insurance Market Evolve*, ABA INS. COVERAGE LITIG., Mar.-Apr. 2014, *available at* http://tinyurl.com/qggwpkv.

[3] *See id.*; Michael Lipkin, *Anthem Data Breach Spawns Email Phishing Scam*, LAW360 (Feb. 6, 2015, 9:41 PM), *available at* http://tinyurl.com/oz62kvh.

[4] Podolak, *supra* note 2; *see also Cyber Risk*, NAIC, http://tinyurl.com/ohcsj4u (last updated Feb. 13, 2015).

data, trade secrets, financial records, and litigation information. Hacking and malicious intrusions are usually the cause of the breach, but human error is just as prevalent a concern."[5] A 2014 study by the Ponemon Institute found that, globally, fifty-nine percent of all breaches are caused by some form of human error—inadequate data security, system glitches, and simple, routine carelessness (like losing an unencrypted company laptop).[6]

Data breaches are so pervasive and costly that 2013 was dubbed the year of the "Mega Breach."[7] There was a sixty-two percent increase in the total number global of breaches from 2012 to 2013 that resulted in the exposure of 552 million identities.[8] The average cost of a malicious data breach in the United States during that timeframe? *$7,155,402*.[9]

The risk continues to evolve not only in sum, but in substance as well. The now routine interconnectivity of multiple systems across all industries has led to the problem of interdependent security risks,[10] and a potentially immeasurable loss exposure. The Target data breach, for example, was initiated through the hack of one of Target's vendors, an HVAC contractor, who was electronically connected to Target for billing purposes.[11] To that end, data thieves constantly look to exploit mundane, seemingly innocuous conduits of information "such as mobile devices (through mobile malware and text messaging phishing schemes), security cameras, smart televisions, automobiles, and even baby

---

[5] Podolak, *supra* note 2; PONEMON INST., 2014 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 8 (2014), *available at* http://tinyurl.com/qyk9tyw; *Cyber Risk*, *supra* note 4.

[6] PONEMON INST., *supra* note 5, at 8.

[7] 19 SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 5 (2014), *available at* http://tinyurl.com/pfm5ogh.

[8] *Id.*

[9] *See* PONEMON INST., *supra* note 5, at 2, 5 (average cost per compromised record ($246) multiplied by average number of breach records (29,087)).

[10] *See* Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1, 9 (2014) ("[W]hat makes cyber-risk management so unpredictable is the interdependency of cyber-risks among firms doing business within the marketplace. Because the security of consumer data relies on interdependent risks in a networked system, the information security risks which one firm faces will depend not only on that firm's own security protocols but also the protocols of others with whom that firm's network is linked. This phenomenon of a single security event in one insured's system affecting that insureds peers—even if those peers are under different administrative control—has been called interdependent security risk." (footnotes omitted)).

[11] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, KREBS ON SECURITY (Feb. 12, 2014), http://tinyurl.com/oab53g7.

monitors."[12] If events in 2014 (already being called another year of Mega Breaches), and the first quarter of 2015, are any indication, this trend will only continue—even though C-Suite[13] executives are increasingly sensitive to the risk:[14]

> RETAIL: Home Depot (September 2014), 56 million customer records (credit/debit cards) breached following hack that affected approximately 2200 stores.[15]
> HEALTHCARE: Anthem (January/February 2015), 80 million customers and employees affected (exposure of names, social security numbers, income data, and email addresses).[16]
> ENTERTAINMENT: Sony Pictures (November 2014), tens of thousands of employees affected when their personal information was leaked online; unreleased movies, executives' salaries, and private emails were leaked online as well.[17]
> FINANCIAL: JP Morgan Chase (August 2014), 76 million records involving names, address, phone numbers, and emails for account holders were breached, plus information on approximately 7 million small businesses.[18]
> INSURANCE: AIG's Variable Annuity Life Insurance Company (February 2014) disclosed that a former financial advisor had taken a hard drive with information related to 774,723 customers.[19]

---

[12] Podolak, *supra* note 2; SYMANTEC CORP., *supra* note 7, at 7.

[13] *C-Suite*, INVESTOPEDIA, http://tinyurl.com/8f8lq7w (last visited Feb. 22, 2015) ("A widely-used slang term to collectively refer to a corporation's most important senior executives.").

[14] PONEMON INST., 2014: A YEAR OF MEGA BREACHES (2015), *available at* http://tinyurl.com/ljlvfqh.

[15] *See* Nandita Bose, *Home Depot Confirms Security Breach Following Target Data Theft*, REUTERS (Sept. 9, 2014, 12:07 PM), http://tinyurl.com/n2oap8e; Anne D'Innocenzio, *Home Depot Breach Affected 56M Debit, Credit Cards*, AP NEWS (Sept. 18, 2014, 10:25 PM), http://tinyurl.com/px3s8eo; Brian Krebs, *Home Depot: 56M Cards Impacted, Malware Contained*, KREBS ON SECURITY (Sept. 18, 2014), http://tinyurl.com/l8pj836.

[16] Lipkin, *supra* note 3.

[17] *Sony Pictures CEO Had 'No Playbook' for Mega-Hack on Studio*, N.Y. TIMES (Jan. 9, 2015, 1:42 AM), http://tinyurl.com/nheqcmk.

[18] *See* Michelle Meyers & Seth Rosenblatt, *JP Morgan: 76M Households Exposed in CyberBreach*, CNET (Oct. 2, 2014, 3:52 PM), http://tinyurl.com/nh4mkme.

[19] *See* Podolak, *supra* note 2; Ellen Messmer, *The Worst Security SNAFUs this Year (So Far!)*, NETWORK WORLD (July 15, 2014, 4:15 AM), http://tinyurl.com/loncnfg.

LEGAL: McKenna Long & Aldridge (2014), software placed on a vendor's system led to a breach of "names, address[es], wages, taxes and Social Security number information contained on federal wage and tax statement form W-2; date of birth, age, gender and ethnicity data; and visa, passport or federal Form I-9F documents numbers . . . ."[20] The law firm is offering all affected individuals one year of free credit monitoring and identity theft protection.[21]
CONSTRUCTION/MANUFACTURING: AECOM (July 2014), Hackers infiltrated company network and stole the records of former and current employees.[22] Boeing/Lockheed Martin (July 2014), Chinese hackers stole sixty-five gigabytes of data on numerous military projects, including trade secrets relating to Boeing's C-17 transport plane and Lockheed Martin's F-22 and F-35 fighter jets.[23]
GOVERNMENT: Internal Revenue Service (March 2014), employee took home personal information on about 20,000 individuals stored on a thumb drive and loaded it onto an unsecure home network.[24]

A. Defining "Cyber Risks"

Cyber Risks cause both first-party losses, those suffered directly by the affected individual or company, and third-party liability claims, which are brought by others against the compromised individual or company.[25] "First-party losses typically include forensic investigation expenses, replacement costs for hardware and/or software, and business interruption losses."[26] In 2013, businesses in the United States suffered

[20] Allison Grande, *McKenna Long Employees' Data Exposed In Vendor Hack*, LAW360 (Mar. 24, 2014), http://tinyurl.com/kosugoo.
[21] *Id.*
[22] *See Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://tinyurl.com/p48jcp9 (last visited Jan. 23, 2015).
[23] Edvard Pettersson, *Chinese Man Charged in Plot to Steal U.S. Military Data*, BLOOMBERG (July 12, 2014, 12:01 AM), http://tinyurl.com/oj2b7ep; *Chronology of Data Breaches*, *supra* note 22.
[24] Messmer, *supra* note 19.
[25] Podolak, *supra* note 2; *see also* Bailey, *supra* note 10, at 11; Lawrence A. Gordon et al., *A Framework for Using Insurance for Cyber-Risk Management*, COMM. ACM, Mar. 2003, at 81, 83.
[26] Podolak, *supra* note 2; *see also* Bailey, *supra* note 10, at 11; Gordon et al., *supra* note 25, at 83.

an average of $3.32 million in lost business costs resulting from data breaches.[27] Data breaches also typically result in direct first-party costs "associated with providing notice of a breach, credit monitoring, public relations consultants, payment of fines and penalties, and compliance with governmental or regulatory investigations."[28] Forty-seven states have security breach notification laws when certain types of PII have been compromised.[29]

Cyber Risks "can also result in a variety of individual and class action third-party liability claims for property damage, invasion of privacy, bodily injury, and/or emotional distress."[30] Consider the real life examples involving Home Depot and Anthem, unfolding as the digital ink dries on this article. The first news report of the Home Depot breach came on Tuesday, September 2, 2014.[31] By the time Home Depot formally confirmed the breach on Monday, September 8, 2014,[32] two consumer class action suits had already been filed in Georgia Federal District Court (a mere fifteen miles from Home Depot's Atlanta-based headquarters).[33] One week later, on September 16, 2014, First Choice Federal Credit Union also filed a class suit in Georgia Federal District Court on behalf of similarly situated financial institutions alleging, among other things, that Home Depot failed to take adequate security measures in the face of multiple highly publicized data breaches occurring across the country.[34] Anthem first detected its breach on

---

[27] PONEMON INST., *supra* note 5, at 16.

[28] Podolak, *supra* note 2; *see also* PONEMON INST., *supra* note 5, at 3.

[29] *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 3, 2014), http://tinyurl.com/nrb9bs7; *see generally* SAXE DOERNBERGER & VITA, P.C., CYBER RISK: SECURITY BREACH NOTIFICATION STATUTES, *available at* http://tinyurl.com/mdguzc7 (last visited Feb. 18, 2015) (survey of states with statutes requiring notification, as of Sept. 11, 2014).

[30] Podolak, *supra* note 2; Kim Zetter, *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*, WIRED (Jan. 8, 2015, 5:30 AM), http://tinyurl.com/o66xv6t (discussing two confirmed cases "in which a wholly digital attack caused physical destruction of equipment"); *see also* Bailey, *supra* note 10, at 13–15.

[31] *See, e.g.*, Brian Krebs, *Banks: Credit Card Breach at Home Depot*, KREBS ON SECURITY (Sept. 2, 2014), http://tinyurl.com/kejxezl.

[32] Press Release, The Home Depot, Inc., The Home Depot Provides Update on Breach Investigation (Sept. 8, 2014), *available at* http://tinyurl.com/ouxb45s.

[33] *See* Complaint, Mazerolle v. The Home Depot, Inc., No. 1:14-cv-02887-WSD (N.D. Ga. Sept. 8, 2014); Complaint, Solak v. The Home Depot, Inc., No. 1:14-cv-02856-WSD (N.D. Ga. Sept. 4, 2014).

[34] *See* Complaint at 3–4, First Choice Fed. Credit Union v. The Home Depot, Inc., No. 1:14-cv-02975-AT (N.D. Ga. Sept. 16, 2014).

January 27, 2015.[35] By February 9, 2015, four lawsuits had already been filed across the country, each seeking in excess of $5 million in damages.[36] For both, the number of liability claims is only likely to grow.[37] One need only look at Target Corporation, which, in November 2014, celebrated the one-year anniversary of its highly publicized breach: more than 140 lawsuits, including 111 consumer-based actions and 29 by banking institutions and/or credit unions.[38]

Privacy breaches also usually result in claims or investigation by various branches of government.[39] Following the Home Depot breach, several Senators pushed for an aggressive investigation by the Federal Trade Commission:[40]

> In response to overwhelming consumer exposure, federal oversight is increasing and becoming increasingly complex. The Federal Trade Commission (FTC) leads the regulatory charge, routinely pursuing claims of "unfair or deceptive" practices affecting commerce against companies that fail to provide adequate data security. The FTC's authority in the cyber arena is only expanding.[41]

---

[35] Elizabeth Weise, *First Lawsuits Launched in Anthem Hack*, USA TODAY (Feb. 8, 2015, 6:07 PM), http://tinyurl.com/lnbk5eo. As is often the case, however, it appears the hackers may have accessed Anthem's systems long before the detection—nine months. Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 9, 2015), http://tinyurl.com/qa8whyo.

[36] Larry Rulison, *Anthem Facing First Lawsuits*, TIMESUNION (Feb. 9, 2015, 8:36 PM), http://tinyurl.com/p845cr5 ("The first lawsuits, each of which seeks in excess of $5 million, were filed in federal courts in Indiana, Alabama, California and Georgia, although it is possible more may be filed in other states in the coming days.").

[37] *See* David Allison, *Home Depot Now Facing 21 Class-Action Lawsuits Over Data Breach*, ATL. BUS. CHRON. (Oct. 13, 2014, 6:25 PM), http://tinyurl.com/mf87l6n (stating that recent figures have the number of pending lawsuits at twenty-one).

[38] Tom Webb & Nick Woltman, *100 Lawyers in a Room: Target Case Draws the Suits to St. Paul*, TWINCITIES.COM (May 14, 2014, 12:01 AM), http://tinyurl.com/n6jpm8v.

[39] *See, e.g.*, Martha Kessler, *Attorneys General Launch Multistate Home Depot Data Breach Investigation*, BLOOMBERG BNA (Sept. 15, 2014), http://tinyurl.com/o8cm7sy.

[40] Teri Robinson, *Markey, Blumenthal Pen Letter to FTC Over Home Depot Breach*, (Sept. 9, 2014), http://tinyurl.com/n2o2ma3.

[41] Podolak, *supra* note 2; *see also What We Do*, FED. TRADE COMMISSION, http://www.ftc.gov/about-ftc/what-we-do (last visited Jan. 23, 2015); FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J.) (holding that recent data-security legislation actually complements and does not restrict the FTC's authority), *motion to certify app. granted*, 2014 WL 2812049, Civ. Action No. 13–1887 (ES) (D.N.J. June 23, 2014).

Although many FTC targets choose to settle out of court, as Facebook famously did in 2011,[42] one company recently disputed the FTC's authority to police data security issues. Before a New Jersey Federal District Court, Wyndham Worldwide Corporation argued that Congress never intended the FTC to have data security oversight and that various other statutory schemes that specifically address the issue should govern.[43] In its April 7, 2014 ruling, the court disagreed with Wyndham and refused to carve out a data security exception from the FTC's province, holding that subsequent data-security legislation actually complements the FTC's authority.[44]

III. INSURANCE POLICY FORM EVOLUTION

To fully appreciate the significance of current litigation trends involving insurance for Cyber Risk and, most importantly, what those trends tell us about the future, one must understand the mechanics of insurance policy form development. Insurance policy language develops during a long process of testing and market reaction born out of case law. Consider, for example, that Commercial General Liability (CGL) policies are primarily sold using standardized forms crafted by Insurance Services Office, Inc. (ISO).[45] These forms are the product of a calculated process that involves evaluating market conditions, relevant legislation and case law, and general industry concerns.[46] As one commentator described, ISO's drafting process closely resembles the passage of legislation:

> First, a perceived problem arises. Second, the drafter learns of the problem through constituent lobbying or the notoriety of an event reflecting the problem. Third, the drafter (ISO and its core "membership" of insurers) considers the problem and interest group sentiment and responds as best it can

---

[42] *See FTC Approves Final Settlement With Facebook*, FED. TRADE COMMISSION (Aug. 10, 2012), http://tinyurl.com/pd4z57q.

[43] *Wyndham*, 10 F. Supp. 3d at 611.

[44] *Id.* at 613.

[45] 1 JEFFREY W. STEMPEL, STEMPEL ON INSURANCE CONTRACTS § 4.05[A], at 29 (3d ed. 2014) (stating that ISO is a private trade association of the property-casualty insurance industry that, through the use of committees and subcommittees, drafts and revises standard form property and casualty policies).

[46] *See* Jeffrey W. Stempel, *The Insurance Policy as Statute*, 41 MCGEORGE L. REV. 203, 213 (2010) (noting that ISO acts like a private legislature for the insurance industry, and standard insurance forms issued by ISO resemble statutory products of legislatures or administrative rules of government agencies).

> consistent with the drafter's assessment of overall interests, including self-interest. Fourth, the drafter issues a response, usually in the form of new or revised policy language.[47]

Steps one and two are usually the result of written judicial opinions interpreting key words, phrases, or clauses in a way that at least one of the parties to the insurance policy contract did not anticipate. Case law, however, does not develop overnight. In fact, it can often take many years for a court to be presented with a situation that requires written interpretation of disputed language. First, a claim must occur that implicates the policy and disputed language. The policyholder and insurer take differing positions and each attempt to leverage their legal position and business relationship to cost-effectively resolve the disagreement. Litigation only becomes an option after informal attempts at negotiation have been exhausted and, even then, numerous considerations—largely financially driven—can still derail a lawsuit. The potential for a written decision increases once a suit is filed, but the debate still must lend itself to motion practice, which requires the court to interpret and apply relevant law (such as a motion to dismiss or for summary judgment). If a factual dispute exists that precludes such a dispositive motion, or the parties settle early, there will never be a need for such a decision. Written opinions, therefore, are generally more the exception than the rule.

To illustrate, consider the evolution of the blanket additional insured endorsement used in CGL insurance. "Additional Insured" coverage is the inclusion of one party on the insurance policy of another, and has been a staple of basic contractual risk transfer for nearly thirty years.[48] Prior to the development of standardized Additional Insured coverage, a party gaining Additional Insured status usually would only

---

[47] *Id.* at 210; *see also* STEMPEL, *supra* note 45, § 4.05[A], at 30 (stating that the drafting process typically results in the production of various materials that reflect on the drafting history, such as memoranda, correspondence, committee meeting minutes, and testimony, which, taken together, "provide a rich source of information potentially shedding light on disputed insurance policy terms"). These materials can be useful in coverage negotiations, as "[c]onsideration of the background of the policy does not do violence to traditional contract language focusing on the text of the document. Often, that text can only be well understood in light of the background and drafting history of the contract. This is particularly true for the standardized, legislation-like contracts that are insurance policies." *Id.*

[48] *See Additional Insured*, IRMI, http://tinyurl.com/pq5rrvp (last visited Jan. 23, 2015) (defining additional insured as "[a] person or organization not automatically included as an insured under an insurance policy who is included or added as an insured under the policy at the request of the named insured").

have an insurable interest in the First Named Insured's insurance, not actual "insured" status, and thus, sometimes cloudy, debatable access to the policy.[49]

The insurance market called for a better approach. Among the first endorsements to provide Additional Insured status, ISO Form 20 10 11 85 gave a party Additional Insured status for any liability "arising out of" the work of the subject policy's First Named Insured.[50] At the time, the "arising out of" language was virtually untested by courts in either this or a similar context. Over the course of the next twenty years, numerous disputes arose across the country regarding the threshold required by this language for the Additional Insured party to access coverage. Carriers argued that "arising out of" required negligence on the part of the First Named Insured or that Additional Insured coverage required a showing that the First Named Insured was negligent[51] or that coverage was limited to vicarious liability.[52] Courts typically sided with policyholders, concluding that a plain reading of "arising out of" required only that the alleged liability of the Additional Insured party "flow from" or "have origins" in the First Named Insured's work.[53] The market reacted and, in 2004, ISO modified the triggering language from "arising out of" to "caused, in whole or in part,"[54] which, in turn, has spawned its own body of litigation.[55]

---

[49] *See generally* S. Tippecanoe Sch. Bldg. Corp. v. Shambaugh & Son, Inc., 395 N.E. 2d 320 (Ind. Ct. App. 1979).

[50] INS. SERVS. OFFICE, INC., FORM CG 20 10 11 85 (1985); Ellen Chapelle, *The Evolution of Additional Insured Endorsements*, GOULD & RATNER (Feb. 26, 2014), http://tinyurl.com/orndwgv.

[51] *See, e.g.*, Cas. Ins. Co. v. Northbrook Prop. & Cas. Ins. Co., 501 N.E. 2d 812, 815 (Ill. App. Ct. 1986) (holding Additional Insured status did not require a showing of negligence because nothing in the policy language so limited coverage).

[52] *See, e.g.*, Phila. Elec. Co. v. Nationwide Mut. Ins. Co., 721 F. Supp. 740, 742 (E.D. Pa. 1989).

[53] *See* Shell Oil Co. v. AC&S, Inc., 649 N.E.2d 946, 951–52 (Ill. App. Ct. 1995) (holding that "'arising out of'" means "'having its origin in,'" "'growing out of,'" and "'flowing from'"); Pro Con Constr., Inc. v. Acadia Ins. Co., 794 A.2d 108, 110 (N.H. 2002) ("The phrase 'arising out of' has been interpreted as meaning 'originating from or growing out of or flowing from.'"); Meadow Valley Contractors, Inc. v. Transcon. Ins. Co., 2001 UT App 190, ¶ 14, 27 P.3d 594 (stating that "'[t]he phrase arising out of is equated with origination, growth, or flow from the event and has much broader significance than caused by'" (alteration in original) (internal quotation marks omitted)).

[54] *See* INS. SERVS. OFFICE, INC., FORM CG 20 10 07 04 (2004).

[55] *See, e.g.*, Gilbane Bldg. Co. v. Admiral Ins. Co., 664 F.3d 589, 592–98 (5th Cir. 2011) (interpreting "'caused, in whole or in part . . .'" to require proximate causation); Pro Con, Inc. v. Interstate Fire & Cas. Co., 794 F. Supp. 2d 242, 256–57 (D. Me. 2011) (including the language "'in whole or in part'" in the Additional Insured clause to evince a specific intent for

A. The Insurance Market Expands Coverage to Include Electronic-Related Publications

ISO has taken a similar approach in modifying the standard form CGL policy to address coverage for electronic-related publications of otherwise private information.[56] Today, the coverage available in an ISO standard CGL policy form is divided into three main parts: (1) Coverage A: Bodily Injury and Property Damage Liability; (2) Coverage B: Personal and Advertising Injury Liability; and (3) Coverage C: Medical Payments.[57]

The current definition of "personal injury" under Coverage B, which is routinely at issue in data/privacy breach coverage disputes, was first incorporated into the ISO CGL form in 1986.[58] At that time, coverage for privacy offenses was limited to "[o]ral or written publication of material that violates a person's right of privacy . . . ."[59] In 2001, in response to an evolving technological landscape and the increased presence of electronic media, ISO broadened the language to its current form: "Oral or written publication, *in any manner*, of material that violates a person's right of privacy . . . ."[60] ISO explained the modification in this way: "[ISO] updated the definition of personal and advertising injury to reference publications 'in any manner' to address *Internet and electronic* publications, and their impact on personal and advertising injury offenses which may arise from publication via e-mail or a website."[61]

"coverage for additional insureds to extend to occurrences attributable in part to acts or omissions by both the named insured *and* the additional insured"); Dale Corp. v. Cumberland Mut. Fire Ins. Co., Civ. A. No. 09-1115, 2010 WL 4909600, at *5 (E.D. Pa. Nov. 30, 2010).

[56] *See* Podolak, *supra* note 2 (detailing the amendments to definitions and coverage exclusions since 2001).

[57] *See*, *e.g.*, INS. SERVS. OFFICE, INC., FORM CG 00 01 12 07, at 1–9 (2006) [hereinafter ISO FORM 2006].

[58] *See* Kyle Lambrecht, *The Evolution of the Advertising Injury Exclusion in the Insurance Service Office, Inc.'s Comprehensive General Liability Insurance Policy Forms*, 19 CONN. INS. L.J. 185, 189 (2012) (stating that prior to the 1986 revision, a policyholder was required to purchase separate ISO CGL endorsements for both "advertising injury" and "personal injury" coverage).

[59] INS. SERVS. OFFICE, INC., FORM CG 00 01 07 98, at 12 (1997).

[60] INS. SERVS. OFFICE, INC., FORM CG 00 01 10 01, at 14 (2000) (emphasis added).

[61] TRACEY WALLER, INS. SERVS. OFFICE, INC., 2012 GENERAL LIABILITY MULTISTATE FORMS REVISIONS ANNOUNCED; PROPOSED 2013 IMPLEMENTATION 14 (2012) (emphasis added).

As industry analysts have discussed, "[a]s part of the 2001 ISO CGL revision, the phrase 'in any manner' was inserted into the . . . invasion of privacy (offense 'e') paragraph[] of the definition, presumably to emphasize the wide range of media in which offensive materials may be 'published.'"[62] IRMI further explains:

> In the age of Internet commerce and vast interconnected electronic databases that store health, financial, legal, and other personal information, "violation of a person's right of privacy" can result from breaches of these databases and either the inadvertent or the criminal dissemination of the electronically stored information. Businesses that store customers' financial information electronically—credit card numbers, for example—face a particular exposure in this connection and *could face liability claims asserting a lack of diligence in keeping such information from falling into the wrong hands*. These data breaches would seem to fall reasonably within the personal and advertising injury definition of "oral or written publication, *in any manner*" of private information, and resulting claims have been paid as losses stemming from a personal and advertising injury offense.[63]

This language was specifically engineered to encompass the type of liability many policyholders now face in our increasingly digital world—"liability claims asserting a lack of diligence in keeping such information from falling into the wrong hands."[64]

IV. CYBER RISK INSURANCE LITIGATION

The insurance market is now going through a similar process with cyber coverage, as it attempts to transition the majority of the risk from traditional lines to a dedicated product. The difference, however, is that this process is not occurring slowly; it will not take twenty years for key concepts in stand-alone cyber insurance to be litigated, they are being litigated right now, and most people don't know it.

---

[62] *Personal and Advertising Injury*, IRMI, http://tinyurl.com/m6o8m6e (last visited Oct. 15, 2014). International Risk Management Institute is a leading commentator on insurance and risk management issues and is well recognized as an independent organization that "researches and analyzes commercial liability provisions for the insurance industry." West American Ins. Co. v. Tufco Flooring E., Inc., 409 S.E.2d 692, 696 (N.C. Ct. App. 1991), *overruled by* Gaston Cnty. Dyeing Mach. Co. v. Northfield Ins. Co., 351 N.C. 293, 524 S.E.2d 558 (2000).

[63] *Personal and Advertising Injury*, *supra* note 62 (first emphasis added).

[64] *See id.*

A. Current Issues in Commercial General Liability

CGL insurance is the most common type of coverage found in corporate insurance programs and policyholders naturally look to CGL as a first source of recovery. The problem: CGL insurers don't view CGL insurance as intending to cover Cyber Risks and they vigorously deny owing any obligation for them.[65] Over the years, the debate has produced litigation on two key fronts: whether there is "property damage"[66] or "personal injury."[67]

For example, there was property damage where a power outage knocked out computer systems for an entire day and caused a loss of data and software functionality in *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc*.[68] Similarly, there was property damage to a computer in *Eyeblaster, Inc. v. Federal Insurance Co.* where the computer froze up and became essentially inoperable.[69] In *America Online, Inc. v. St. Paul Mercury Insurance Co.*, however, software and data were not "tangible property" and any "loss of use" (the secondary definition of "property damage") was excluded.[70] Finally, an internet service provider's interception and internal dissemination of its users' online activities for advertising purposes qualified as personal injury (breach of privacy) in *Netscape Communications Corp. v. Federal Insurance Co.*[71]

---

[65] Scott Godes & Jennifer G. Smith, *Insurance for Cyber Risks: Coverage Under CGL and "Cyber" Policies*, ABA SEC. OF LITIG. 6–7 (Mar. 1–3, 2012), *available at* http://tinyurl.com/pgcpjvm.

[66] The standard CGL Coverage A insuring agreement provides: "We will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage' to which this insurance applies." ISO FORM 2006, *supra* note 57, at 1. Prior to the 2001 ISO form, "property damage" meant, in relevant part, "[p]hysical injury to tangible property" and "[l]oss of use of tangible property that is not physically injured." INS. SERVS. OFFICE, INC., FORM CG 00 01 10 93, at 12 (1992). Since 2001, the definition further provides that "electronic data is not tangible property." ISO FORM 2006, *supra* note 57, at 15.

[67] The Coverage B insuring agreement provides: "We will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury' to which this insurance applies." ISO FORM 2006, *supra* note 57, at 6. "'Personal and advertising injury'" means, among other things, "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." *Id.*

[68] Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185 TUC ACM, 2000 WL 726789, at *1–*2, *4 (D. Ariz. Apr. 18, 2000).

[69] Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 801–02 (8th Cir. 2010).

[70] Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 92, 94–96 (4th Cir. 2003).

[71] *See, e.g.*, Netscape Commc'ns Corp. v. Federal Ins. Co, 343 F. App'x. 271, 272 (9th Cir. 2009); *see also* Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., No. CCB-06-2055, 2007

B. Courts Debate "Publication"

Although claims involving coverage for "property damage" and "bodily injury" routinely arise, today's dialogue for Cyber Risk CGL coverage has largely centered on a multitude of issues surrounding whether there has been a "publication" that triggers the "personal and advertising" coverage.[72]

1. Does compromised information constitute a "publication"?

The Connecticut Supreme Court is poised to take the lead on a critical question pertaining to Cyber Risk coverage under a CGL policy: Under what circumstances does a data breach constitute a "publication"? With briefing recently completed, oral arguments will soon take place for *Recall Total Information Management v. Federal Insurance Co.*,[73] where a third-party storage vendor lost 130 IBM data tapes that included unencrypted personal information for 500,000 past and present IBM employees.[74] The tapes literally "fell out of the back of [a] van" while in transit, were taken by an unknown person (witnessed by a New York Department of Transportation worker), and never recovered.[75] IBM incurred $6 million for costs and expenses resulting from the loss of the tapes—notification to affected individuals, establishing a call center for inquiries, credit monitoring, and credit restoration.[76] Recall Total Information Management, the vendor, reimbursed IBM and pursued

---

WL 3268460, at *5 (D. Md. Oct. 26, 2007) (holding that under the CGL policy's advertising injury definition, "publication" did not need to be divulged to a third party, the perpetrators' wrongful access to the information was sufficient).

[72] *See, e.g.*, Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC, No. 1:13-cv-917 (GBL), 2014 WL 3887797, at *2 (E.D. Va. Aug. 7, 2014); Recall Total Info. Mgmt., Inc., v. Fed. Ins. Co., 147 Conn. App. 450, 462–64 (2014), *cert. granted*, 311 Conn. 925 (2014); Transcript of Order at 28–29, 32–33, Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Ct. Mar. 10, 2014) (No. 526).

[73] Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 311 Conn. 925 (2014) (granting cert.).

[74] *Recall*, 147 Conn. App. at 453–54.

[75] *Id.*; Brief for Appellant at 2, Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 147 Conn. App. 450, *cert. granted*, 311 Conn. 925 (Mar. 5, 2014) (SC 19291) ("[A] New York Department of Transportation ('NYDOT') worker who had been called to investigate debris on the highway observed a Caucasian male loading the wheeled cart, which contained 130 of the IBM tapes, into a white pick-up truck. The driver of the pickup truck lied to the NYDOT worker by falsely claiming that the cart and tapes were his." (citations omitted)).

[76] *Recall*, 147 Conn. App. at 454 & n.3.

CGL coverage.[77] The insurers, Federal Insurance Co. and Scottsdale Insurance Co., denied the claim, arguing that "publication" requires a showing of "access," and because there was no evidence anyone "accessed" the information on the tapes there was no "publication."[78]

The insurers were able to convince the Connecticut Appellate Court of their position,[79] but the argument should fail before the Connecticut Supreme Court. The Appellate Court's conclusion that there was no publication appears to have been unaffected by the fact that IBM was legally required to take action under relevant state security breach notification laws (laws that are generally intended to address the scenario where private information is no longer private), because it reasoned that such statutes can be triggered by the need for preventative action and that such statutes do not necessarily reflect that a privacy breach has actually occurred.[80] This logic is flawed, however, as state privacy breach notification statutes are fundamentally concerned with the threat of exposure, i.e., a publication.

As a technical matter of contract interpretation and construction, Recall correctly argued that "publication" does *not* require "access" in this context, and that the theft of the unencrypted tapes qualifies.[81] Neither insurer defined the word "publication," and the word "access" is not used in conjunction with the insuring agreement in either policy. In fact, "access" does not appear anywhere in the Federal policy.[82] Courts interpreting the term publication, in the privacy breach context, have repeatedly adopted a broad interpretation.[83] Recall was entrusted with

[77] *Id.* at 458. Recall was an Additional Insured, see *supra* notes 48–55 and accompanying text, on a CGL policy procured by its subcontractor, Executive Logistics. *Id.* at 453. Recall also pursued a contractual indemnity claim against Executive Logistics and, after the insurers denied coverage, acquired Executive Logistics' rights under the policy. *Id.* at 454.

[78] *See* Reply Brief for Appellant at 2–10, Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 147 Conn. App. 450, *cert. granted*, 311 Conn. 925 (Mar. 5, 2014) (SC 19291).

[79] *See* Recall Total Info. Mgmt., Inc., v. Fed. Ins. Co., 147 Conn. App. 450 (2014).

[80] *See id.* at 464 ("[M]erely triggering a notification statute is not a substitute for a personal injury.").

[81] *See* Brief of Plaintiff-Appellants at 20–21, Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 147 Conn. App. 450, *cert. granted*, 311 Conn. 925 (Mar. 5, 2014) (SC 19291).

[82] *See* Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., No. X07CV095031734S, 2012 WL 469988, at *5 (Jan. 17, 2012).

[83] *See* Melrose Hotel Co. v. St. Paul Fire & Marine Ins. Co., 432 F. Supp. 2d 488, 503 (E.D. Pa. 2006) (stating that publication "can include the simple act of issuing or proclaiming"), *aff'd sub nom.* Subclass 2 of Master Class of Plaintiffs Defined & Certified in Jan. 30, 2006 & July 28, 2006 Orders of Circuit Court of Cook Cnty., Ill. in Litig., 503 F.3d 339 (3d Cir. 2007); Encore Receivable Mgmt., Inc. v. ACE Prop. & Cas. Ins. Co., No. 1:12-CV-297, 2013 WL 3354571, at *8–*9 (S.D. Ohio July 3, 2013) (the mere recording of a

the care of the exclusive representation of the IBM employee information in the corporeal world—the data tapes.[84] It is the transfer of the tapes to someone not entrusted with their protection that is simultaneously the source of the breach of privacy and a "*publication* of material that . . . violates a person's right of privacy."[85]

A New York trial court's analysis of this issue sheds some light. In *Zurich American Insurance Co. v. Sony Corp. of America*, hackers compromised Sony's PlayStation Network and stole consumer personal information.[86] There was no allegation or evidence that the thieves further disseminated the stolen information:

> [INSURANCE COMPANY COUNSEL]: When we are talking about [whether] the insured published anything, we are assuming that the underlying complaints are alleging that the hackers published something. But, it doesn't allege that.
>
> . . . .
>
> The plaintiffs are only alleging that *they have a fear that the hackers may do so*. But, there is no allegation that the hackers themselves published anything.
>
> THE COURT: That is getting into real subtleties. Because, I look at it as a Pandora's box. Once it is opened it doesn't matter who does what with it. It is out there. It is out there in the world, that information. And whether or not it's actually used later on to get any benefit by the hackers, that in my mind is not the issue. The issue is that it was in their vault. Let's just say to visualize this,

---

conversation by a customer service call center, without any evidence of further dissemination, constituted a publication that triggered CGL coverage because the initial dissemination of the speech, from the speaker's mouth to the recording device, was a publication because the speaker was being deprived of the ability to control the communication; no evidence of access of the recording was required), *appeal dismissed*, (6th Cir. May 8, 2014), *vacated*, (May 19, 2014).

[84] "One cannot escape the fact that software, recorded in physical form, becomes inextricably intertwined with, or part and parcel of the corporeal object upon which it is recorded, be that a disk, tape, hard drive, or other device." S. Cent. Bell Tel. Co. v. Barthelemy, 94-0499, p. 13 (La. 10/17/94); 643 So. 2d 1240, 1247 (analyzing taxation of software as physical property); *see also* Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 738 (Minn. Ct. App. 1991) (finding CGL coverage for the loss of a computer tape and its data under Coverage A as "property damage" and reasoning, "[b]ecause data can be removed from a computer tape at any time, the transfer of the physical property (the tape) is only incidental to the purchase of the knowledge and information stored on the tape. Thus, the tape has little value for tax purposes. *But if the tape is lost while it still contains the data, as is the case here, its value is considerably greater*." (emphasis added) (citation omitted)).

[85] Recall Total Info. Mgmt., Inc., v. Fed. Ins. Co., 147 Conn. App. 450, 462 (2014) (omission in original).

[86] *See* Transcript of Order at 31–32, Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Ct. Mar. 4, 2014) (No. 525). The court did not issue a written decision in that case; the court's decision is contained in a transcript and excerpted *infra* note 88 and accompanying text.

> the information was in Sony's vault. Somebody opened it up. It is now, this comes out of the vault. But, whether or not it's actually used that is something, that's separate. On the one hand it is locked down and sealed. But, now you have opened it up. You cannot ignore the fact that it's opened for everyone to look at.[87]

In summarizing its position on the issue, the court again focused on the exposure of the information, regardless of form, from a secure location:

> THE COURT: In this case here I have a situation where we have a hacking, an illegal intrusion into the defendant Sony's secured sites where they had all of the information. That information is there. It's supposed to be safeguarded. That is the agreement that they had with the consumers that partake or participated in that system. So that in the box it is safe and it is secured. Once it is opened, it comes out. And this is where I believe that's where the publication comes in. It's been opened. It comes out. It doesn't matter if it has to be oral or written. We are talking about the internet now. We are talking about the electronic age that we live in. *So that in itself, by just merely opening up that safeguard or that safe box where all of the information was, in my mind my finding is that that is publication. It's done.*[88]

Legislative efforts by the insurance industry involving personal and advertising injury coverage confirm that this is the correct outcome. In addition to leaving "publication" undefined, the insurance industry acknowledges that the "in any manner" language was specifically crafted to encompass these types of exposures (as discussed above in Section III).[89] The insurance market now is trying to scale back available coverage by modifying relevant forms. In April 2013, ISO created a brand new endorsement,[90] the sole purpose of which is to allow insurance companies to delete the entire "publication, in any manner" definition of personal and advertising injury.[91] ISO confirms that the modification is "a restriction in coverage," and other commentators have recognized that this change would undermine coverage for data breach

---

[87] *Id.* at 41–42 (emphasis added).

[88] *Id.* at 76–77 (emphasis added).

[89] *See* WALLER, *supra* note 61, at 49.

[90] An endorsement is an insurance policy form added onto the base form used to construct the policy that changes, adds to, or subtracts from the provisions in that base form. *Endorsement*, IRMI, http://tinyurl.com/lsq64xh (last visited Jan. 25, 2015).

[91] INS. SERVS. OFFICE, INC., FORM CG 24 13 04 13 (2012); WALLER, *supra* note 61, at 14.

claims:[92] "ISO members have grown increasingly concerned about privacy claims, particularly with respect to the internet. Possibly in an effort to funnel such claims to media and [other stand-alone] cyber policies, the markets are pushing back on privacy claims [submitted] under the GL policy."[93]

In May 2014, ISO also made available an exclusion specifically designed to eliminate coverage for breach of privacy liability, excluding personal and advertising injury

> arising out of any access to or disclosure of *any person's* or organization's *confidential or personal* information, including . . . financial information, credit card information, health information or any other type of nonpublic information. This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss . . . arising out of any access to or disclosure of any person's . . . confidential or personal information.[94]

The enumerated damages are those customarily associated with data breach claims and, indeed, are precisely the damages at issue in *Recall*: (1) notification of the affected individuals; (2) staffing and maintaining call centers for the affected individuals; and (3) providing credit monitoring and credit restoration services.[95]

If the endorsement deleting the "publication, in any manner" definition is the nail, this new exclusion is the Gallagher mallet[96] that closes the coffin on the debate of whether data breach coverage is included in the personal and advertising injury insuring agreement of the prior ISO form and standard CGL policies. If the coverage did not exist, the new exclusion would be superfluous, and it is a fundamental tenet of insurance policy contract analysis that words and phrases will not be

---

[92] The endorsement "entirely eliminates in the first instance the key definition that is the 'hook' for the data breach coverage under the CGL Coverage B . . . ." Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 TORT TRIAL & INS. PRAC. L.J. 529, 566 (2014).

[93] MARSH & MCLENNAN COS., 2013 CHANGES TO ISO ENDORSEMENTS 6 (2013), *available at* http://tinyurl.com/ms2vp4m.

[94] INS. SERVS. OFFICE, INC., FORM CG 21 06 05 14 (2013) (emphasis added).

[95] Brief of Plaintiff-Appellants at 3, Recall Total Info. Mgmt., Inc., v. Federal Ins. Co., 147 Conn. App. 450, *cert. granted*, 311 Conn. 925 (Mar. 5, 2014).

[96] An informal survey among my peers suggests this may be a reference lost on many readers. If that is the experience of this reader, I highly recommend, for your own benefit, an immediate internet search. *See* Craig Marquardo, *Geico Commercial Featuring Gallagher*, YOUTUBE (July 12, 2012), http://tinyurl.com/l3t99ap.

interpreted so as to render them meaningless.[97] In *R.T. Vanderbilt Co. v. Hartford Accident & Indemnity Co.*, the court analyzed the historical significance of the creation of an asbestos exclusion as evidencing that coverage—absent the exclusion—is available for such losses,[98] and stated:

> [T]he very adoption of separate asbestos exclusions in policies beginning in 1986 *is in itself evidence* that the insurance industry did not consider the pollution exclusion language to be clear enough to exclude such claims. To argue the pollution exclusion was unambiguous and therefore excluded asbestos related claims would render the asbestos exclusion redundant and unnecessary. Consequently, the [insurers] have failed to meet their burden of demonstrating the applicability of the standard and absolute pollution exclusions in their policies.[99]

Simply put, if the insurers are correct that the personal and advertising injury coverage does not apply, these modifications would not be necessary.

Another critical decision from 2014, published in the midst of the *Recall* briefing, and which should pave the way for a policyholder victory in *Recall*, is *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC*.[100] In *Portal*, a Virginia Federal District Court (applying Virginia law) confirmed CGL coverage for claims

---

[97] *See, e.g.*, Clark Sch. for Creative Learning, Inc. v. Phila. Indem. Ins. Co., 734 F.3d 51, 56 (1st Cir. 2013) ("'Every word in an insurance contract must be presumed to have been employed with a purpose and must be given meaning and effect whenever practicable.'"); Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Willis, 296 F.3d 336, 339 (5th Cir. 2002) ("[C]ourts are to ensure the policy is interpreted in such a way as to give effect to each term in the contract so that none will be rendered meaningless."); Beister v. John Hancock Mut. Life Ins. Co., 356 F.2d 634, 641 (8th Cir. 1966) ("Another rule for construction of contracts is that interpretations should be sought that give meaning to all parts of the contract, and interpretations which render meaningless parts of the contract should be avoided."); Czapski v. Maher, 954 N.E.2d 237, 244 (Ill. App. Ct. 2011) ("An interpretation that renders a provision meaningless is not reasonable."); Cty. of Columbia v. Cont'l Ins. Co., 634 N.E.2d 946, 950 (N.Y. 1994) ("[I]t is settled that in construing an endorsement to an insurance policy, the endorsement and the policy must be read together, and the words of the policy remain in full force and effect except as altered by the words of the endorsement. . . . An insurance contract should not be read so that some provisions are rendered meaningless." (citations omitted)).

[98] R.T. Vanderbilt Co. v. Hartford Accident & Indem. Co., No. X02UWYCV075016321, 2014 WL 1647135, at *2–*4 (Conn. Super. Ct. Mar. 28, 2014).

[99] *Id.* at *29 (emphasis added).

[100] Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC., No. 1:13-cv-917 (GBL), 2014 WL 3887797 (E.D. Va. Aug. 7, 2014).

where confidential medical information was made available online—*even though* there was no evidence anyone ever viewed the information.[101] Portal specializes in the electronic safekeeping of medical records for hospitals, clinics, and other medical providers, including hosting certain records on electronic servers.[102] Several patients of a New York hospital discovered that their records were available on the internet after stumbling across them during a basic Google search of their own names; these patients then initiated a class action suit against Portal for failing to safeguard their information.[103] Portal turned to its CGL insurer, Travelers, for defense and indemnity.[104] Travelers responded by denying coverage, and then filed a declaratory judgment action against Portal.[105] Travelers and Portal both moved for summary judgment.[106]

In ruling for Portal, the court held that the presence of information online amounts to a "publication."[107] The court reasoned that "publication" requires only that information be "placed before the public," and that the mere availability of the information online is sufficient, regardless of whether it's ever accessed or viewed by anyone.[108] Echoing the court's discussion in the Sony decision, *supra*, the *Portal* court opined, "the definition of 'publication' does not hinge on third-party access. . . . By Travelers' logic, a book that is bound and placed on the shelves of Barnes & Noble is not 'published' until a customer takes the book off the shelf and reads it."[109]

The same logic should apply in *Recall*. Once the data tapes fall outside Recall/Ex Log's exclusive control, the information can no longer be safeguarded and is considered published. It is irrelevant whether the tapes now reside in the hands of one person or a hundred people, or whether any effort has been made to access the information on the tapes. The tapes and the information are, at this very moment no less, out of the safe box and on the shelf at Barnes & Noble and, therefore, published.

---

[101] *Id.* at *6.
[102] *Id.* at *1.
[103] *Id.* at *1–*2.
[104] *Portal*, 2014 WL 3887797, at *1.
[105] *Id.* at *2.
[106] *Id.*
[107] *Id.* at *5.
[108] *Portal*, 2014 WL 3887797, at *4.
[109] *Id.* at *4–*5.

2. Who has to commit the publication?

Another important decision slated for opinion during 2015 is *Zurich American Ins. Co. v. Sony Corp. of America*.[110] Sony is seeking CGL "personal injury" coverage following a hack of its PlayStation Network, which resulted in stolen personal information belonging to 100 million users.[111] Zurich contends that the relevant policy language "oral or written publication in any manner of the material that violates a person's right of privacy" requires the publication be made by the insured.[112] Because hackers stole the information, Zurich argues, there is no publication by Sony and thus no coverage.[113]

In its February 21, 2014 ruling from the bench, the trial court sided with Zurich.[114] The decision, appealed on April 9, 2014, was surprising given that (1) the relevant language makes no mention of *who* must make the publication (to the contrary, "any manner" will suffice) and (2) the underlying class action suit against Sony specifically alleged that Sony's lax security measures permitted the hackers to gain access to the network, meaning that Sony arguably *was responsible for the publication* and at least should be entitled to a defense from Zurich. Not surprisingly, the court told the parties at the onset of its ruling that the insurance issues were important enough to require "immediate Appellate authority."[115]

3. The collection of information is not publication.

In *National Union Fire Insurance Co. of Pittsburgh, PA v. Coinstar*, a Washington Federal District Court held that a CGL insurer was not obligated to defend two class action lawsuits alleging the

---

[110] *See* Chad Hemenway, *Sony Appeals Ruling in CGL case with Zurich, Mitsui*, ADVISEN (Apr. 17, 2014), http://tinyurl.com/mynmu8s; Jeff Sistrunk, *Insurance Cases to Watch in 2015*, LAW 360 (Jan. 2, 2015, 3:19 PM), http://tinyurl.com/mn5lzys.

[111] Luke Quinlan, *New York Trial Court Denies Coverage for Cyber Claims Under Commercial General Liability Policies*, MCGUIRE WOODS (Mar. 4, 2014), http://tinyurl.com/pbpv4lh.

[112] Transcript of Order at 29, 52, Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Ct. Mar. 4, 2014) (No. 525).

[113] *Id.* at 9.

[114] *Id.* at 80 ("In this case my finding is that there was no act or conduct perpetrated by Sony, but it was done by 3rd party hackers illegally breaking into that security system. And that alone does not fall under paragraph E's coverage provision.").

[115] *Id.* at 81; Bibeka Shrestha, *Sony Fights Ruling That Nixed Data Breach Coverage*, LAW360 (Apr. 11, 2014), http://tinyurl.com/owyydr4.

collection and distribution of personal information in violation of privacy statutes in Michigan and California.[116] In the second class action, the *Mehrens* lawsuit, the underlying plaintiffs alleged that Redbox had violated California's Song-Beverly Credit Card Act by collecting customers' billing zip code and/or email at the time of the transaction.[117] The *Mehrens* plaintiffs further alleged that Redbox used this information for its own marketing and sold it to third parties.[118] The Song-Beverly Act prohibits an entity from requesting or requiring that a cardholder provide information when accepting a credit card payment.[119] Redbox argued that the allegations that information was sold to third parties triggered coverage for injury "'arising out of' the '[o]ral or written publication, in any manner, of material that violates a person's right of privacy.'"[120] The court disagreed, reasoning that the only harm claimed by the *Mehrens* plaintiffs stemmed from the violation of the Song-Beverly Act, which focuses on the collection of information, not its publication.[121]

4. Statutory violation exclusions are not necessarily implicated simply because the government is involved.

Given the considerable government interest in regulating privacy violations and data security, insurers have also been denying coverage on exclusions relating to statutory violations. Such was the case before a California Federal District Court in *Hartford Casualty Insurance Co. v. Corcino & Associates*, where Stanford Hospital sought coverage for litigation brought by numerous patients alleging privacy rights violations.[122] The underlying plaintiffs alleged that Stanford and others posted confidential medical information on a public website in violation

[116] Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Coinstar, Inc., No. C13-1014-JCC, 2014 WL 3891275, at *7 (W.D. Wa. Aug. 7, 2014).

[117] *Id.* at *6.

[118] *Id.*

[119] *Id.*

[120] *Coinstar*, 2014 WL 3891275, at *6 (alteration in original).

[121] *Id.* In a partial win for Redbox, however, the court held that National Union was responsible for the payment of all reasonable defense costs up to the time the court determined that it did not owe a duty to defend. *Id.* at *8. The court held that because National Union explicitly agreed to allow Redbox to select defense counsel and failed to set forth the rates it was willing to pay in the policy or reservation of rights letters, National Union could not subsequently limit the rates it would pay to defend the underlying actions. *Id.*

[122] Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF (JCx), 2013 WL 5687527, at *1 (C.D. Cal. Oct. 7, 2013).

of their constitutional privacy rights and California's Confidentiality of Medical Information Act.[123] The plaintiffs also claimed statutory damages under California's Welfare and Institutions Code.[124]

The CGL policy at issue covered "electronic publication of material that violates a person's right of privacy," but excluded any such injury "[a]rising out of the violation of a person's right to privacy created by any state or federal act."[125] The exclusion contained an exception, however, for "liability for damages that the insured would have in absence of such state or federal act."[126] After examining the relevant legislative history, the court held that the exception to the exclusion applied; thus, the policyholder was entitled to coverage because the statutes at issue did not create new privacy rights, but merely codified and created an enforcement mechanism for existing rights.[127]

The Federal District Court for the Western District of Washington faced a similar dispute in *National Union Fire Insurance v. Coinstar*.[128] In its ruling, the court held that alleged violations of the Video Privacy Protection Act (VPPA)[129] fell within an exclusion for "'any act that violates any statute . . . that addresses or applies to the sending, transmitting or communicating of any material or information, by any means whatsoever.'"[130] Specifically, the underlying plaintiffs had alleged that Coinstar retained customers' PII it had obtained through its Redbox system and used that data for marketing purposes, as well as disclosing the information to third parties without the customers' express permission.[131] The court found the exclusion unambiguous and that it applied to the alleged VPPA violations.[132]

The plaintiffs, in a separate class action heard by the same court in August 2014, alleged that Redbox violated Michigan's Video Protection Privacy Act, which prohibits the distribution of customer information

---

[123] *Id.* at *1–*2.
[124] *Id.* at *2.
[125] *Id.* at *2–*3.
[126] *Corcino*, 2013 WL 5687527, at *3.
[127] *Id.* at *5–*6.
[128] *See* Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Coinstar, Inc., No. C13-1014-JCC, 2014 WL 868584 (W.D. Wash. Feb. 28, 2014).
[129] The VPPA, codified at 18 U.S.C. § 2710, "'prohibits a "video tape service provider" from disclosing [to any person] "personally identifiable information" about one of its consumers.'" *Id.* at *3 (alteration in original).
[130] *Id.* (omission in original).
[131] *Id.* at *1.
[132] *Coinstar*, 2014 WL 868584, at *3.

related to the purchase or rental of books, sound recordings and video records, by disclosing customer information collected at rental kiosks to third parties.[133] The court held that these claims were excluded as liability arising out of the violation of a statute that "'addresses or applies to the sending, transmitting or communicating of any material or information . . . .'"[134] Many data breach/cyber risk claims are statutorily based and CGL insurers routinely contend this exclusion applies, although its application on a case-by-case basis should be fact specific.

Both rulings may be anomalous, as many versions of the exclusion addressed in the latter *Coinstar* case are specifically limited to violations involving the Telephone Consumer Protection Act,[135] CAN-SPAM,[136] and the Fair Credit Reporting Act.[137] In fact, Coinstar attempted to argue for this more narrow scope, but was unsuccessful only because the relevant policy period was not so specifically limited.[138] With that in mind, the Washington Federal Court's decisions provided two important Cyber Risk lessons for policyholders: (1) given the prominence of government intervention in data breach losses, insurers may attempt to take advantage of any exclusion pertaining to statutory violations; and (2) at the time of renewal, policyholders should take care to avoid unnecessarily broad exclusions pertaining to statutory violations or government regulations.

5. Stay tuned, there's more to come.

With three prominent cases likely to add to the debate over the next few years, Cyber Risk CGL litigation shows no signs of slowing down. First, security firm Red Coats, Inc., d/b/a Admiral Security Services, Inc. is taking the debate to the Eleventh Circuit Court of Appeals following an adverse ruling before a Florida Federal District Court, arguing that the theft of laptops with unencrypted, sensitive information triggers both

[133] Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Coinstar, Inc., No. C13-1014-JCC, 2014 WL 3891275, at *2 (W.D. Wa. Aug. 7, 2014).

[134] *Id.* at *4.

[135] 47 U.S.C. § 227 (2012).

[136] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701–13 (2012).

[137] 15 U.S.C. § 1681 (2012).

[138] Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Coinstar, Inc., No. C13-1014-JCC, 2014 WL 868584, at *3 (W.D. Wash. Feb. 28, 2014).

"property damage" and "personal and advertising injury" coverage.[139] Admiral was hired by healthcare provider, AvMed, Inc., to provide onsite security services at AvMed's premises in Gainesville, Florida,[140] however, "one of Admiral's security guards stole three [laptops] containing HIPAA-protected personal information" for an estimated 1.22 million AvMed members.[141] AvMed sued Admiral to recover the resulting notification, credit monitoring, loss of reputation, and litigation expenses,[142] which presumably included AvMed's reported $3 million settlement with the class.[143] Admiral sought various forms of insurance, including CGL from Carolina Casualty Insurance Company, who denied coverage.[144] Citing to *Portal* on appeal, Admiral correctly argued that the theft of the laptops and information, much as is in *Recall*, constituted a "publication" that triggered coverage.[145]

From approximately May 2013 to January 2014, Michaels Stores, Inc. was the victim of a hacking event that resulted in the exposure of as many as three million customer credit and debit cards.[146] Class action litigation followed and, in June 2014, Michaels' CGL insurer, Safety National Casualty Corporation, filed a declaratory judgment action against Michaels seeking to disclaim coverage.[147] Safety National alleged, among other things, that the data breach does not qualify as "personal and advertising injury."[148]

In October 2014, P.F. Chang's China Bistro, Inc.'s CGL insurer, Travelers, filed a coverage-based lawsuit in Connecticut Federal District

---

[139] Initial Brief of Appellant at 31, Red Coats, Inc. d/b/a Admiral Sec. Servs., Inc. v. Carolina Cas. Ins. Co., 2014 WL 4129322, (11th Cir. Aug. 18, 2014) (No. 14-12002-F).

[140] *Id.* at 3.

[141] *Id.* at 2 (stating, in the appellant's initial brief, that the original estimate put the number of stolen records in the thousands); *AvMed Health Plans*, PRIVACY RIGHTS CLEARINGHOUSE, http://tinyurl.com/n39namc (last visited Jan. 25, 2015) (listing the current estimate, as of Nov. 16, 2010, at 1.22 million).

[142] Initial Brief of Appellant at 4, Red Coats, Inc. d/b/a Admiral Sec. Servs., Inc. v. Carolina Cas. Ins. Co., 2014 WL 4129322 (11th Cir. Aug. 18, 2014) (No. 14-12002-F).

[143] *See AvMed Health Plans*, *supra* note 141.

[144] Initial Brief of Appellant at 6, Red Coats, Inc. d/b/a Admiral Sec. Servs., Inc. v. Carolina Cas. Ins. Co., 2014 WL 4129322, (11th Cir. Aug. 18, 2014) (No. 14-12002-F).

[145] Interestingly, the District Court's brief opinion never addressed the "publication" debate, although Admiral's Eleventh Circuit brief indicates that the point was argued. *Id.* at 46.

[146] Elizabeth A. Harris, *Michaels Stores' Breach Involved 3 Million Customers*, N.Y. TIMES (Apr. 18, 2014), http://tinyurl.com/mvncbn8.

[147] Ronald A. Sarachan & Zoë K. Wilhelm, *Cybersecurity: Litigation, Crime & Enforcement*, DRINKERBIDDLE (Aug. 7, 2014), http://tinyurl.com/qeouqqk.

[148] *Id.*

Court.[149] In June 2014, the news first broke[150] that the restaurant chain had been the subject of a breach involving approximately seven million customer credit/debit cards from thirty-three stores in eighteen states over a period of nine months.[151] Several consumer class action lawsuits soon followed, and on October 2, 2014, Travelers filed suit seeking to avoid coverage for all of them.[152] Among the various defenses to coverage that Traveler's raised in its complaint: the breaches did not trigger the "personal and advertising injury" coverage.[153] A decision on this argument could come as soon as the end of 2015/early 2016, as the parties recently agreed to a two-phased discovery approach that would have dispositive motions filed by October 2, 2015.[154]

C. First Party Insurance May Be Available

1. Property Insurance: Does the policy contemplate electronic losses?

Policyholders are facing coverage disputes on the first-party front as well. On November 21, 2013, a Georgia Federal District Court analyzed first-party property insurance in *Metro Brokers, Inc. v. Transportation Insurance Co.*[155] In *Metro Brokers*, a real estate broker's (Metro) online banking system was hacked by a thief who fraudulently authorized Automated Clearing House payments from one of Metro's client escrow accounts to several banks throughout the United States.[156] Metro's first-party property insurance covered "direct physical loss of or damage to Covered Property . . . caused by or resulting from a Covered

---

[149] *See* Matthew Sturdevant, *Travelers Says Liability Policy Doesn't Cover P.F. Chang's Data Breach*, HARTFORD COURANT (Oct. 10, 2014, 10:28 AM), http://tinyurl.com/m5blx56.

[150] *See, e.g.*, Brian Krebs, *Banks: Credit Card Breach at P.F. Chang's*, KREBS ON SECURITY (June 10, 2014), http://tinyurl.com/k8kvee7.

[151] Jeffrey Roman, *P.F. Chang's Breach: 33 Locations Hit*, DATA BREACH TODAY (Aug. 4, 2014), http://tinyurl.com/muzzxjr.

[152] Sturdevant, *supra* note 149; Declaratory Judgment Complaint at ¶ 3, Travelers Indem. Co. of Conn. v. P.F. Chang's China Bistro, Inc., 2014 WL 5280480 (D. Conn. Oct. 2, 2014) (No. 3:14-cv-01458).

[153] *Id.* ¶ 43.

[154] *See* Docket Report, Travelers Indem. Co. of Conn. v. P.F. Chang's China Bistro, Inc., No. 3:14-cv-01458-VLB (D. Conn. Dec. 19, 2014) (No. 25).

[155] Metro Brokers, Inc. v. Transp. Ins. Co., No. 1:12-CV-3010-0DE, 2013 WL 7117840 (N.D. Ga. Nov. 21, 2013). The same court was involved in the Home Depot class action suit discussed, *supra*, at notes 31–37 and accompanying text.

[156] *Id.* at *1–*2.

Cause Of Loss" and included a coverage extension for "[f]orgery."[157] The policy excluded losses involving "'malicious code'" and "'system penetration.'"[158]

The court found that there was no coverage for two reasons. First, the electronic transfers did not meet the insuring agreement definition of forgery because they did not qualify as "'a check, draft, promissory note, bill of exchange, or similar written promise, order, or direction to pay a sum certain.'"[159] The court characterized the "forgery" definition as applying only to "traditional" negotiable instruments and distinguished the policyholder's loss as involving an electronic transfer.[160] Essentially, the court was drawing a line between physical instruments and those commenced "by the click of a button and a series of electronically transmitted codes."[161] Antiquated definitions such as these, which fail to acknowledge the largely digital atmosphere in which currency exists can be, as illustrated by *Metro*, extremely problematic.

In concluding that the insuring agreement had not been met, the court's analysis could have ended. It went on, however, to discuss the exclusions. Metro had argued: (1) that neither exclusion should apply because the theft was proximately caused by a person (or persons); and (2) that the computer virus was merely a tool those person(s) used to commit the theft.[162] Unfortunately, the exclusions, which the court described as "extraordinarily broad," were preceded by anti-concurrent language[163] that effectively defeated Metro's argument.[164]

Nonetheless, as the corporeal and digital worlds increasingly overlap as a result of the prevalence of technological infrastructure, cyber-related events may result in traditional physical damage, which should be covered as a first-party property loss. For example, in 2014, hackers compromised the control systems of a German steel mill, resulting in massive physical damage to a blast furnace.[165] The insurance

---

[157] *Id.* at *1.
[158] *Id.*
[159] *Metro Brokers*, 2013 WL 7117840, at *5.
[160] *Id.*
[161] *Id.*
[162] *Id.* at *6.
[163] A clause customarily seen in first-party policies that is intended to exclude a loss even when caused by a combination of both covered and excluded causes of loss. *Anti-concurrent Cause (ACC) Provision*, IRMI, http://tinyurl.com/p8m3mwm (last visited Jan. 25, 2015).
[164] *Metro Brokers*, 2013 WL 7117840, at *6.
[165] Zetter, *supra* note 30.

response has not been disclosed, but without a carefully orchestrated program, there could easily be a wide gap in coverage.

2. Crime Insurance: Common data breach damages are proximately caused by hacking.

In 2012, the Sixth Circuit Court of Appeals considered whether the theft of credit card information from a retailer is covered under Crime Insurance. In *Retail Ventures, Inc. v. National Union Fire Insurance Co.*, hackers used DSW's local wireless network to access DSW's main computer system and download credit card and checking account information of 1.4 million customers from 108 stores.[166] DSW suffered losses relating to customer communications, public relations, customer claims and lawsuits, and attorney's fees in connection with state and federal investigations (including the FTC).[167] DSW sought $6.8 million from AIG under the "Computer Fraud Rider" of its Crime Insurance.[168] The Rider insured loss "resulting directly from" the theft of insured property by computer fraud.[169]

In its attempt to deny coverage, AIG first argued that the "resulting directly from" language should be interpreted narrowly to mean "sole[ly]" or "immediate[ly]," thus precluding coverage for the majority of DSW's damages.[170] The court disagreed and applied a proximate cause standard, agreeing with the district court that "'there is a sufficient link between the computer hacker's infiltration of Plaintiffs' computer system and Plaintiffs' financial loss'" to trigger coverage.[171]

AIG also argued that the loss was excluded as "loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind."[172] The court disagreed and held that the stolen customer information was not DSW's confidential information, but was obtained from customers in order to receive payment, and did not involve the manner in which the business was

[166] Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821, 824 (6th Cir. 2012).

[167] *Id.*

[168] *Id.* at 824. The total losses of $6.8 million were made up of $5.3 million in stipulated losses incurred by the plaintiffs, plus $1.49 million in pre-judgment interest. *Id.* at 825.

[169] *Retail Ventures*, 691 F.3d at 825.

[170] *Id.* at 828.

[171] *Id.*

[172] *Id.* at 832.

operated.[173] Since the loss was not "clearly excluded," DSW was entitled to coverage.[174]

V. CYBER INSURANCE

A. Cyber Risks Are Being Pushed Out of Traditional Lines

In addition to aggressively denying coverage under traditional lines, the insurance market is continuing its effort to modify standard coverage terms to prospectively eliminate the debate. ISO amended the definition of property damage to specifically omit coverage for "electronic data" in 2001, and in 2014 also added an exclusion for "[d]amages arising out of the loss of, loss of use of, damage to, corruption or, inability to access, or inability to manipulate electronic data."[175] Although courts generally interpret exclusions narrowly, "arising out of" is usually broadly defined.[176] Importantly, ISO offers an endorsement that carves damages because of property damage to electronic data out of the exclusion;[177] the 2013 form also excludes bodily injury claims.[178] Similar "electronic" exclusions are also becoming mainstays of property policies; electronic data is often specifically identified as excluded "property."[179] And, as discussed above in Section IV, ISO has recently created endorsements that substantially narrow "personal and advertising injury" coverage (CG 24 13 04 13) and broadly exclude claims involving the access or disclosure of confidential personal information (CG 21 067 05 14).[180] These modifications will pose a considerable hurdle to obtaining CGL coverage for Cyber Risks and the savvy policyholder must carefully scrutinize its insurance policies to see if they are included.

---

[173] *Retail Ventures*, 691 F.3d at 834.

[174] *Id.*

[175] BRITTON D. WEIMER ET AL., CGL POLICY HANDBOOK § 2.01, at 4 (2d ed. 2014 Supp.); Craig F. Stanovich, *The New ISO Commercial General Liability Policy: A Summary of December 2004 Policy Changes*, IRMI (Oct. 2004), http://tinyurl.com/pzto6jd.

[176] R. Steven Rawls & Robert J. Witmeyer, *"Arising Out of": How Strong is the Connection?*, IRMI (Aug. 2010), http://tinyurl.com/ozarvae.

[177] INS. SERVS. OFFICE, INC., FORM CG 04 37 12 04 (2003).

[178] INS. SERVS. OFFICE, INC., FORM CG 04 37 04 13 (2012).

[179] *See* Donald S. Malecki, *Risk Management—Electronic Data Exclusion*, ROUGH NOTES, http://tinyurl.com/kf9g4dp (last visited Jan. 25, 2015).

[180] *See supra* notes 91–94 and accompanying text.

B. Dedicated Cyber Lines Need Careful Examination

"[T]here has been a significant increase in stand-alone cyber policies hitting the marketplace."[181] In general, these are viable, common-sense alternatives to traditional policies, but the market is immature in many respects. "In fact, 'cyber insurance' has only existed since the late 1990s, when the focus was primarily on Y2K conversion concerns."[182] While ISO has created a product,[183] there is no standard form; thus, the vast majority of products are in manuscript form ("some 50–70 different insurers are writing policies"),[184] and the essential language can vary dramatically. Coverage usually can include "website publishing, security breach liability, programming errors and omissions, replacement of electronic data, and business income."[185] Some policies cover only first-party losses, while others cover only third-party losses; some may provide defenses, although some only indemnity.[186]

Although there are many new concepts incorporated into these policies that have yet to be tested by courts, current Cyber Risk litigation under traditional lines actually offers insight into the future of related coverage debates and policy modifications.

1. The "access" problem.

In *Recall*, Federal Insurance Company contends: (1) "publication" in the data/privacy breach context means "access" and (2) that facts akin to those in *Recall* do not demonstrate "access"—a position openly endorsed by several prominent insurance company trade associations.[187]

---

[181] Podolak, *supra* note 2; *see, e.g.*, *CyberRisk*, TRAVELERS, http://tinyurl.com/knotedb (last visited Jan. 25, 2014).

[182] Podolak, *supra* note 2; *see, e.g.*, Anna Lee, *Why Traditional Insurance Policies are not Enough: The Nature of Potential E-Commerce Losses & Liabilities*, 3 VAND. J. ENT. L. & PRAC. 84, 88 (2001); Rainer Böhme & Galina Schwartz, Modeling Cyber-Insurance: Towards a Unifying Framework 1 (May 21, 2010) (working paper), *available at* http://tinyurl.com/mt5ms8k.

[183] *ISO's Cyber Liability Insurance Program*, VERISK ANALYTICS, http://tinyurl.com/kdbcnl2 (last visited Jan. 25, 2014).

[184] Podolak, *supra* note 2.

[185] *Id.*

[186] *Id.*

[187] *See* Brief of Amici Curiae, Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 147 Conn. App. 450, *cert. granted*, 311 Conn. 925 (Mar. 5, 2014) (SC 19291). Trade Associations contributing to the amici brief include: The American Insurance Association, Complex

Although that particular debate takes place in the CGL context, it is imperative to recognize that many cyber insurers have embedded this same hotly debated concept into dedicated Cyber Risk products, which could lead to considerable debate and unexpected coverage denials.

The Chubb Group of Insurance Companies (affiliated with Federal) offers a CyberSecurity Coverage Part, in conjunction with its ForeFront Portfolio 3.0 program, which includes coverage for "Privacy Notification Expenses" resulting from "Disclosure Liability" which, in turn, is premised on a showing of "potential or actual *access*."[188] The Cyber Suite Insurance Policy from Liberty International Underwriters insures "Notification Expenses," and requires "actual or suspected, unauthorised *access* by a **Third Party** or **Employee** to personally identifiable information."[189] Beazley's Information Security and Privacy Insurance with Electronic Media Liability insures PII that "was *accessed* or reasonably may have been *accessed*" and defines a "Security Breach" as including "the gaining of *access* to or use of **Computer Systems**."[190]

Some policies also use qualifying language (e.g. "potential," "suspected," "reasonably"), suggesting a more expansive interpretation that should support a finding of coverage in a *Recall*-type situation. It cannot, however, be overlooked that insurance carriers are using the CGL litigation forum to strategically advocate a narrow interpretation of "access," a term that, apart from endorsements, appears nowhere in standard form CGL policies. If successful, those arguments may seriously call into question whether dedicated policies are appropriately designed.

2. Evolving statutory schemes and the narrow definitions of privacy breach coverage.

A related issue involves including a sufficiently expansive definition of PII or PHI to reflect the constant evolution of data breach security and notification laws. Some policies define covered PII by

Insurance Claims Litigation Association, and Property Casualty Insurers Association of America.

[188] CHUBB GROUP OF INS. COS., FORM 14-02-17276 1, 3 (2010), *available at* http://tinyurl.com/nkvm63t (emphasis added).

[189] LIBERTY INT'L UNDERWRITERS, CYBER SUITE INSURANCE POLICY 13 (2012) (first emphasis added).

[190] BEAZLEY, FORM F00106SL 11, 15–16 (2011), *available at* http://tinyurl.com/ndgpmpa (last emphasis in original).

reference to specific statutory schemes and/or regulations. At one point in 2014, twenty-three states were either introducing or revising privacy breach legislation.[191] Other states may tie in the concept of "access,"[192] which may not align with all forty-seven state notification statutes and, as extensively discussed in Section III, could be improperly limited by judicial interpretation.

Consider that the Chubb ForeFront Portfolio 3.0 CyberSecurity policy defines "privacy notification expenses" in terms of potential or actual unauthorized access of a person's "record."[193] "Record" is subsequently defined to encompass the traditional forms of personal information—one's first or last name, in combination with a social security number, driver's license number, debit or credit card number, or other personal identification number.[194] Unfortunately, this stagnant definition does not encompass the constantly evolving state of technology and security breach notification laws. For example, Iowa, Kentucky, Nebraska, North Carolina, and Wisconsin incorporate various forms of biometric data into their definitions of "personal information."[195] Thus, if there was a breach of an individual's biometric

---

[191] *2014 Security Breach Legislation*, NCSL (Dec. 23, 2014), http://tinyurl.com/l9r6p8s.

[192] BEAZLEY, *supra* note 190, at 11 (defining Breach Notice Law as "any United States federal, state or territory statute or regulation that requires notice to persons whose **Personally Identifiable Non-Public Information** was *accessed* or reasonably may have been *accessed* by an unauthorized person." (first emphasis in original)).

[193] CHUBB GROUP OF INS. COS., *supra* note 188, at 6.

[194] *Id.*

[195] IOWA CODE ANN. § 715C.1(11) (West, Westlaw through 2014 Reg. Sess.) (defining personal information as "an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual . . . (5) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data"); KY. REV. STAT. ANN. § 365.720(4) (West, Westlaw through end of 2014 Legislation) (defining personally identifiable information as "data capable of being associated with a particular customer through one (1) or more identifiers, including but not limited to . . . fingerprints, photographs or computerized image . . ."); NEB. REV. STAT. ANN. § 87-802(5) (LEXIS through 2014 103rd 2d Sess.) (defining personal information as "a Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements . . . (e) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation"); N.C. GEN. STAT. §§ 75-61(10), 14-113.20(b) (LEXIS through 2014 Reg. Sess.) (defining personal information in conjunction with § 14-113.20(b)(11) which includes in identifying information biometric data); WIS. STAT. ANN. § 134.98(b) (West, Westlaw through 2013 Act 380) (defining personal information as "an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements . . . 5. The individual's unique biometric data,

data, there may not be coverage under the Chubb policy for notification costs because an individual's "record" was not breached.

Other policies, however, such as the Liberty Mutual DataPro Policy, adopt expansive definitions of personal information designed to address the ever-changing nature of data. The DataPro policy includes a catch-all provision, which provides that personal information is "any other information relating to an identified or identifiable natural person who can be identified in particular by reference to an identification number or multiple factors specific to his or her physical, physiological, mental, economic, cultural or social identity."[196]

3. Tension between prior approval and self-effectuating statutes.

Another area rife with inherent tension involves self-effectuating statutes that compel action by a policyholder regardless of any formal claim being commenced (such as security breach notification statutes) and the insurance policy contractual requirement that policyholders not make any "voluntary payments" without the insurance company's prior approval.

An October 2014 decision illustrating this point is *First Commonwealth Bank v. St. Paul Mercury Insurance Co.*, where a Pennsylvania Federal District Court concluded that payments a bank was legally compelled to make pursuant to state statute following the hack of a client's account were not "voluntary."[197] A First Commonwealth Bank client was the victim of a malware attack that allowed a third party to access the client's network.[198] The hacker then obtained the client's Senior Vice President's on-line banking credentials and transferred $3.6 million out of the client's account at First Commonwealth Bank.[199] Pursuant to a Pennsylvania banking statute,[200] First Commonwealth refunded the client's money and subsequently submitted a claim to St.

---

including fingerprint, voice print, retina or iris image, or any other unique physical representation").

[196] LIBERTY SURPLUS INS. CORP., FORM LSI DP P001, at 6 (2013).

[197] First Commonwealth Bank v. St. Paul Mercury Ins. Co., Civ. A. No. 14-19, 2014 WL 4978383, at *4 (W.D. Pa. Oct. 6, 2014).

[198] *Id.* at *1.

[199] *Id.* $76,520 was ultimately recovered and returned to the client. *Id.*

[200] 13 PA. CONS. STAT. ANN § 4A204(a) (West, Westlaw through 2014 Reg. Sess.).

Paul under its professional liability policy.[201] St. Paul denied coverage, arguing that First Commonwealth's payment constituted a voluntary payment.[202] On a motion to dismiss, the court, citing decisions from the United States Supreme Court and a New Jersey Federal District Court, concluded otherwise.[203] The court reasoned that the statute mandated that the payment be made; therefore, the payment was not voluntary.[204]

In addition to arguing that payments of this sort do not qualify as "voluntary," *ab initio*, many jurisdictions preclude an insurer from asserting a "voluntary payment" defense if it has not suffered prejudice.[205] Some cyber insurers are making efforts to undercut these arguments by incorporating more stringent requirements into their policies. For example, some policies systematically incorporate a requirement of "prior written consent" with certain concepts throughout the policy.[206]

4. Potential property damage gaps with CGL coverage.

In most standard form (ISO) CGL policies today, property damage coverage for electronic data losses is limited to those losses that result from physical injury to tangible property, with tangible property being defined so as not to include electronic data.[207] Based on a plain reading of this language, the apparent intent is to preserve coverage for electronic data losses that are caused by property damage, but eliminate the notion that electronic data, in and of itself, can be considered property damage. Cyber policies, conversely, ordinarily exclude

[201] *First Commonwealth Bank*, 2014 WL 4978383, at *1.

[202] *Id.* at *3.

[203] *Id.* at *4.

[204] *Id.*

[205] *See, e.g.*, Truck Ins. Exch. v. Unigard Ins. Co., 94 Cal. Rptr. 2d 516, 524 (Cal. Ct. App. 2000) ("[T]he right to be indemnified cannot relate back to payments made or obligations incurred before notice. . . . The prejudice requirement . . . applies only to the insurer's attempt to assert lack of notice as a *policy defense* against payment even of losses and costs incurred *after* belated notice." (omissions in original); Bond/Tec, Inc. v. Scottsdale Ins. Co., 622 S.E.2d 165, 168 (N.C. Ct. App. 2005) ("[W]e conclude an insurer must show prejudice where the insured has breached the voluntary payments clause of the parties' insurance contract.")).

[206] *See, e.g.*, ACE GROUP, FORM PF-29282, at 5, 9 (2010), *available at* http://tinyurl.com/kt57opo; Sarah Turpin & Roberta D. Anderson, *What to Consider When Buying Cyberinsurance*, RISK MGMT. (Oct. 1, 2014, 6:00 AM), http://tinyurl.com/o5pxbpc ("Cyberinsurance policies include defense provisions that typically limit coverage for defense costs to those that are reasonable and incurred with the insurer's prior written consent.").

[207] *See supra* Part V.A.

coverage for property damage claims.[208] Essentially, the market intends for the two coverage lines to complement one another. Assuming that the parties to the contract agree on this approach, the concept is logical. As with anything that hinges on detail, however, careful execution is critical and many cyber policies employ a much broader exclusion that could result in a coverage gap. For example, Travelers Cyber Risk Policy provides:

> This **CyberRisk Policy** will not apply to any **Claim** or **Single First Party Insured Event** based upon or *arising out of* damage to, or destruction of, loss of, or loss of use of, any tangible property including damage to, destruction of, loss of, or loss of use of, tangible property that results from inadequate or insufficient protection from soil or ground water movement, soil subsidence, mold, toxic mold, spores, mildew, fungus, or wet or dry rot.[209]

Similarly, a Liberty Surplus Insurance Corporation policy excludes claims "based upon, or *arising from* injury to or destruction of any tangible property including loss of use thereof except this exclusion shall not apply to **Claims** arising from **Malicious Code**; for the purposes of this exclusion, *data does not constitute tangible property* . . . ."[210]

Courts interpret the phrase "arising out of" broadly, while interpreting "result from" more restrictively.[211] Theoretically, therefore, an electronic-related loss that has some minimal connection to property damage could be excluded from cyber insurance under the "arising out of" language, yet fail to trigger the CGL definition because the loss does not "result from" property damage.

5. Does the cyber policy contemplate the full scope of damages?

Current case law also suggests that the causal relationship between a cyber-event and the sustained damages will be a source of tension under cyber insurance policies. In *Retail Ventures*, AIG argued that

---

[208] *See supra* Part V.A.

[209] TRAVELERS INDEM. CO., FORM CYB-3001, at 12 (2010) (last emphasis added).

[210] LIBERTY SURPLUS INS. CORP., FORM LSI TI P001, at 12 (2013) (first and last emphasis added).

[211] Spirco Envtl., Inc. v. Am. Int'l Specialty Lines Ins. Co., 555 F.3d 637, 642 (8th Cir. 2009) ("The court held that the language 'resulting from' was more narrow than the language 'arising out of,' but was not so limited as to be synonymous with proximate or immediate causation.").

common data breach losses for customer communications, public relations, customer claims and lawsuits, and attorney's fees related to government investigations were too remotely related to a hacking event to be covered.[212] In *Recall*, Federal and Scottsdale argue to the Connecticut Supreme Court that similar damages—notification costs, call center costs, and monitoring services—are "[c]onsequential."[213] Many cyber policy insuring clauses expressly require that a loss be directly caused by, or solely and directly caused by, an insured cause.[214]

In the Travelers CyberRisk Policy, for example, damages for restoration expenses (i.e., expenses to restore, replace, or reproduce damaged or destroyed computer programs, software or other electronic data stored within a computer system) must be "directly caused" by a "computer violation."[215] Computer violation is defined to include (1) a computer virus that has been "introduced" into a computer system; (2) damage caused by a natural person without authorization; or (3) damage caused by a natural person with authorization who uses said authorization to cause the damage or destruction.[216] Thus, if a computer virus damages a group of files, but as a result all files (including those not damaged) must be restored and reproduced, an insurer with this or similar language may contend replacement expenses for the undamaged files are not covered, under the theory that the damage was not "directly caused" by the computer violation.

6. Governmental regulation exclusions and industry specific concerns.

As the *Coinstar* decisions illustrate, governmental regulation and statutory violations are an increasingly routine aspect of Cyber Risk litigation and related coverage disputes, and will be pursued as a means of denying coverage. In general, this language is difficult to reconcile with the increasingly heavily regulated field of Cyber Risk, but the problem becomes even more acute in particular sectors. For example, one policy that was sold to a financial management company, subject to

[212] Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821, 824, 831 (6th Cir. 2012).

[213] Joint Appellees' Brief at 11, Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 147 Conn. App. 450, *cert. granted*, 311 Conn. 925 (Mar. 5, 2014) (SC 19291).

[214] *See Retail Ventures*, 691 F.3d at 828, 831.

[215] TRAVELERS INDEM. CO., *supra* note 209, at 2.

[216] *Id.* at 5.

regulation by the Securities and Exchange Commission, contains an exclusion for:

> [A]ny actual or alleged violation of any securities law, regulation or legislation, including but not limited to the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Act of 1940, any state or provincial blue sky or securities law, any other federal securities law or legislation, or any other similar law or legislation of any state, province or other jurisdiction, or any amendment to the above laws, or any violation of any order, ruling or regulation issued pursuant to the above laws . . . .[217]

The legal liability for Cyber Risk is rapidly and constantly evolving and policyholders and carriers must take extra care to ensure these products contain appropriate limitations.

7. A moving target, "reasonable" security measures underlie Cyber Risk insurance.

The core purpose of Cyber Risk insurance is to allow an insured to transfer the risk of a breach or compromise of network integrity. It comes as no surprise then that insurers concentrate on the implementation and maintenance of appropriate security and IT protocols as the foundation of coverage. The concept is featured prominently in the technical examination required in most policy applications (representations that are often incorporated directly into the policy itself), as well as a variety of exclusions. Policyholders must examine these procedures and their significance to the policy, or they may face an unanticipated forfeiture of coverage.

For example, inaccurate descriptions of data security measures—even if unintentional—could be used to invalidate coverage under Travelers' CyberRisk Policy, which provides:

> If any statement or representation in the **Application** is untrue, then no coverage will be afforded under this **CyberRisk Policy** . . . . Whether an **Insured Person** had such knowledge will be determined without regard to whether the **Insured Person** actually knew the **Application**, or any other

[217] BEAZLEY, *supra* note 190, at 7.

> application completed for this **CyberRisk Policy**, contained any such untrue statement or representation.[218]

The referenced application contains many detailed questions regarding information security and personnel policies, any of which could lead to a loss of coverage if answered inaccurately.[219] A few examples include:

- "Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company?"[220]
- What is the frequency of security audits and "[i]s anti-virus software installed on *all* of the **Applicant's** computer systems, including laptops, personal computers, and networks?"[221]

The Allied World Assurance Company Privacy Liability and Network Risk Insurance Policy excludes "**Business Interruption Costs** caused directly or indirectly by any failure of an **Insured** to continuously implement the procedures and risk controls identified in the **Application**."[222]

Even where an insured follows the industry standard for information security, it is very possible, in light of emerging technologies, that the industry standard itself will be considered negligent or unreasonably insecure. Before the Target breach, no one would fathom requiring an HVAC contractor to maintain security measures similar to those of Target. With Fazio Mechanical serving as the gateway for that breach, however, the line is getting blurred.

The trend of increased public scrutiny on industry standards for data security continues. As of this writing, Anthem believes that a hacker group using a stolen employee password broke into its files.[223] Although Anthem was required to store the social security numbers and personal data of its members, it was not required to encrypt this

---

[218] TRAVELERS, CYBERRISK INSURING AGREEMENT: CYB-3001, at 22–23 (2010), *available at* http://tinyurl.com/nzkdhz9.

[219] TRAVELERS, CYBERRISK COVERAGE APPLICATION: CYB-1100-IND, at 2–4 (2010), *available at* http://tinyurl.com/la3naqp.

[220] *Id.* at 3.

[221] *Id.* at 2–3 (first emphasis added).

[222] ALLIED WORLD ASSURANCE CO. (U.S.) INC., PRIVACY LIABILITY AND NETWORK RISK INSURANCE POLICY, FORM PV 00001 00, at 12 (2010).

[223] Danny Yadron & Melinda Beck, *Health Insurer Anthem Didn't Encrypt Data in Theft*, WALL STREET J. (Feb. 5, 2015, 7:26 PM), http://tinyurl.com/m3h7gab.

information, making it more easily accessed by intruders.[224] According to Anthem, non-encryption is the industry standard.[225] At the same time, the standard is changing, as New Jersey recently passed legislation requiring such data to be encrypted.[226] Whether non-encryption amounts to negligence, failure to mitigate damages, or both, what effect that has on coverage is certain to play out in the coming years.[227]

Although there is no single governing standard for the reasonableness of security procedures, and certain industries are subject to more exacting standards than others, there are several common factors that merit careful consideration.

First, an insured needs to evaluate its information assets. Different information may be subject to different laws and disclosure protocols. After this, the associated risks should be assessed and a protocol for repeated, periodic risk assessment needs to be implemented. Risks should be evaluated in light of the nature of the business, its transactional capabilities, the sensitivity and value of the stored information to the business and its trading partners, and the size and volume of its transactions. This process will provide the baseline against which security measures can be selected, implemented, measured, and validated. After the analysis, a security program must be put into effect with particular emphasis on access through employees and human error. Many of the data breaches discussed in this article were traced back to misplaced laptops, thumb-drives, mobile devices, and passwords.[228]

In addition to monitoring current access and equipment, care must be taken to cancel access that had been granted to former employees and to prevent data breaches through old or disposed-of equipment. For

---

[224] *Id.*

[225] *Id.*

[226] S.B. 562, 216th Leg., Reg. Sess. (N.J. 2014), *available at* http://tinyurl.com/lpt274u.

[227] There may be a systemic disconnect between how secure insurance companies think they are and their actual level of security. According to Benjamin M. Lawsky, Superintendent of the New York Department of Financial Services (NYDFS), "'Recent cyber security breaches should serve as a stern wake up call for insurers and other financial institutions to strengthen their cyber defenses.'" The NYDFS intends on "put[ting] forward enhanced regulations requiring institutions to meet heightened standards for cyber security . . . ." *Id.* This is no surprise considering that the department found that, in the insurance industry, ninety-five percent of insurers believe that they have sufficient information security staffing as is and that only fourteen percent of insurance CEO's receive monthly briefings on information security issues. Press Release, N.Y. DEP'T OF FIN. SERVS., NYDFS Announces New, Targeted Cyber Security Assessments for Insurance Companies (Feb. 8, 2015), *available at* http://tinyurl.com/mda7xek.

[228] *See supra* Section II.

example, many people do not realize that photocopiers generally have hard drives that save images of copied documents.[229] One investigation of used photocopiers offered for sale revealed confidential domestic violence complaints from a police sex-crimes unit and ninety-five pages of a construction company's paystubs, complete with the names, addresses, and social security numbers of its employees.[230] A data breach based on improperly discarding confidential information may be excluded from coverage. To that end, businesses must diligently oversee any third-party service providers and contractually require them to implement appropriate security measures, properly dispose of anything that could contain confidential information or provide network access, and monitor the performance of the outsource providers.

Finally, experienced risk management staff, IT staff, insurance brokers, and coverage counsel should all be involved in evaluating insurance coverage and completing application forms. A seemingly innocent mistake on a policy application, or a precisely worded exclusion, could leave a gaping hole in a business's risk transfer scheme.

VI. CONCLUSION

Insurance coverage for Cyber Risks under traditional coverage lines has been hotly litigated over the last decade, with a bevy of critical decisions taking place in 2014 alone, and with still more to come in 2015. Insurers are increasingly attempting to move Cyber Risks to dedicated policies and, although coverage under traditional policies will be increasingly difficult to access, they may still be available to respond to cyber losses in certain circumstances. Policyholders need to recognize that today's litigation trends will heavily influence the cyber insurance products of tomorrow and plan accordingly.

[229] Armen Keteyian, *Digital Photocopiers Loaded With Secrets*, CBS NEWS (Apr. 19, 2010, 6:12 PM), http://tinyurl.com/lymouuc.

[230] *Id.*