Chapter 16

Insurance for Data Breaches, Cyber Crime, and Unauthorized Privacy Disclosures

Steven R. Gilford

JAMS

Marc E. Rosenthal*

Proskauer Rose LLP

* The authors would like to thank Proskauer associate Michael Wheat and summer associates Ramon Alvarez and Maryam Muhammad for their work researching and updating the current version of this chapter.

§ 16:1 Overview

The unauthorized disclosure of personal and other confidential information has become a well-known and constant risk for holders of third-party information and business data.[1] Notification letters

1. *See, e.g.*, Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/; Charlie Osborne, *The biggest data breaches, hacks of 2021*, ZDNET (Dec. 31, 2021), www.zdnet.com/article/the-biggest-data-breaches-of-2021/; Shelby Brown, *14 of the worst data leaks, breaches, scrapes and security snafus in the last decade*, CNET (Apr. 23, 2021), www.cnet.com/how-to/14-of-the-worst-data-leaks-breaches-scrapes-and-security-snafus-in-the-last-decade/. Well-known companies like Macy's, Capital One, Burger King, Marriott, Zoom, MGM Resorts,

from companies that have suffered data breaches have become commonplace, and high-profile breaches of literally millions of records at major companies have become the subject of headlines and board of directors meetings around the world.[2] In recent years, these risks have increased exponentially by a continuing stream of ransomware attacks in which whole operations of a company are actually or potentially brought to a halt by hackers.[3]

In addition to asserted claims of data privacy breaches, risks from technology exposures include business interruption, extortion demands, inability to perform obligations to others, damage to reputation, and loss or distortion of company and client data. As businesses continue to evolve in a technology-driven environment, so too do practices for the handling and protection of sensitive information and data. Due to the ubiquity and increasing quantity of digital information and operations, information holders are exposed to a multitude of operational and data privacy risks.[4] The costs

---

Facebook, Twitter, DoorDash, LinkedIn, Kroger, Volkswagen, Allstate, Robinhood, and Kronos are only a few of those who experienced data breaches in recent years.

2. *See, e.g.*, Robert R. Ackerman Jr., *Corporate boards are better at cybersecurity but still need improvement*, SEC. MAG. (May 6, 2021); Eve Tahmincioglu, *Report: Cybersecurity Remains a Top Company Threat for Directors* (Dec. 6, 2018), www.directorsandboards.com/news/report-cybersecurity-remains-top-company-threat-directors (noting that while a majority of directors report understanding cybersecurity issues, only 52% report being confident in providing "effective cyber-risk oversight" and 50% being "confident that their companies are secured against a cyber attack"); *Accellion Incident*, KROGER, www.kroger.com/i/accellion-incident; Clifford Krauss, Nicole Perlroth & David E Sanger, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 8, 2021), www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

3. In 2021, over $602 million in payments were attributed to ransomware attacks on companies—$200 million more than the year before—and that figure is likely to be underreported. *The 2022 Crypto Crime Report*, CHAINALYSIS (Feb. 2022), https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

4. Data loss or security breaches can occur in a number of ways, including network hacking, lost or stolen laptops, spyware, phishing, insecure media disposal, hacked card swiping devices, security vulnerabilities on mobile devices, misdirected mail and faxes, insecure wireless networks, peer-to-peer software, breaches in physical security, problematic software updates or upgrades, human error, rogue or disgruntled employees, and lost or stolen media. Even companies that specialize in storing personal information or passwords have been hacked. *See, e.g.*, Andy Meek, *If you use this popular password manager, all of your passwords may have been*

associated with a data breach or unauthorized disclosure of confidential information can be substantial,[5] and they are likely to continue to increase as governmental regulators and the plaintiffs' bar become increasingly vigilant and sophisticated in cyber privacy issues and concerns.[6] At the same time, corporate directors and officers are facing increased exposure to liability, as plaintiffs' attorneys have endeavored to hold them responsible for allegedly inadequate attention to computer and data security.[7]

As the risks associated with data and privacy breaches continue to grow and evolve, companies and individuals have turned, in varying degrees, to their insurers for protection. One report estimated the market for cyber insurance in 2022 at $11.9 billion in gross annual premiums and predicts it to increase to $29.2 billion by 2027.[8] The percentage of companies and individuals purchasing cyber insurance grew from 47% in 2019 to 61% in 2022.[9] At the same time, the cost of cyber insurance is growing quickly, with premiums reportedly rising by 92% in 2021.[10]

---

stolen, BGR (Apr. 27, 2021), https://bgr.com/tech/data-breach-customers-need-to-change-passwords-after-passwordstate-hack-5922020/; Sead Fadilpašić, *Almost half of businesses have suffered a data breach in recent years*, TECHRADAR (Apr. 15, 2022), www.techradar.com/news/almost-half-of-businesses-have-suffered-a-data-breach-in-recent-years.

5. In 2022, the costs of a compromised record reportedly averaged $164 per record globally, and the average cost per data breach event was $4.24 million. Data breaches are most expensive in the United States where the average cost per data breach event was $9.44 million. Cost of Data Breach Report 2022 (July 2022), PONEMON INST. LLC, www.ibm.com/security/data-breach. Costs associated with a typical data breach can include, but are not limited to, internal investigations, forensic experts, consumer notifications, discounts for future products and services, credit monitoring, crisis management, call centers, attorney fees, payment card industry fines, increased processing fees, litigation (including damages, awards and settlements, agency and attorney general actions), reputational costs, and technology upgrades. *Id*.
6. *See infra* sections 16:2.2 and 16:3.3.
7. *See infra* section 16:2.3[A].
8. MarketsandMarkets, *Cybersecurity Insurance Market Worth $29.2 Billion By 2027*, PR NEWSWIRE (June 21, 2022), www.prnewswire.com/news-releases/cybersecurity-insurance-market-worth-29-2-billion-by-2027--exclusive-report-by-marketsandmarkets-301571822.html.
9. Ben Zigterman, *61% Of Organizations Have Cyberinsurance, Survey Finds*, LAW360 (May 27, 2022), www.law360.com/articles/1497721/61-of-organizations-have-cyberinsurance-survey-finds.
10. James Rundle & David Uberti, *Cyber Insurers Raise Rates amid a Surge in Costly Hacks*, WALL ST. J. (May 18, 2022), www.wsj.com/articles/cyber-insurers-raise-rates-amid-a-surge-in-costly-hacks-11652866200.

Historically, claims for insurance for cyber risks have been asserted under traditional coverages, including commercial general liability (CGL) policies, directors and officers (D&O) liability insurance, errors and omissions (E&O) policies, and commercial crime and first-party property and business interruption policies. Insurers, however, have frequently taken the position that these traditional coverages do not cover claims for data and privacy breaches. In addition, in today's market, traditional policies often include specific exclusions aimed at eliminating coverage for cyber risks in their entirety or at least in part.[11]

Given the substantial costs associated with litigating a major coverage case, and the tactical complexities of having to simultaneously deal with claims from a cyber loss and an insurance dispute, businesses have sought more clearly applicable coverages. Insurers have responded by developing insurance products specifically designed to respond to cyber issues with a panoply of names such as network risk policies, cyber insurance, network security liability, privacy liability, and data loss policies.[12] Insurers have also developed

---

11. *See, e.g.*, ISO Endorsement CG 21 07 05 14 (2013) (excluding "(1) [a]ny 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; or (2) the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"); Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 2012 Conn. Super. LEXIS 227, at *17 (Jan. 17, 2012) (definition of property damage provided that "tangible property does not include any software, data or other information that is in electronic form."), *aff'd*, 115 A.3d 458 (Conn. 2015); *see infra* notes 25, 28, 46, and 72. *See generally* 2 STUART A. PANENSKY ET AL., DATA SEC. & PRIVACY LAW § 14:23 (2015) (stating that a recent version of the ISO Commercial General Liability Coverage form specifically excludes electronic data as tangible property in its definition of property damage); Ins. Servs. Office, Inc., Commercial General Liability Coverage Form CG 00 01 10 01, § V (17)(b) (2008), LEXIS, ISO Policy Forms ("For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media . . . .").

12. *See, e.g.*, *CyberFirst*, TRAVELERS, www.travelers.com/cyber-insurance; *DigiTech Enterprise Risk Management*, CHUBB, www.chubb.com/us-en/business-insurance/digitech-enterprise-risk-management-digitech-erm.html *see also* Chubb, CyberSecurity Form 14-02-14874, § I.J. (2009); PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § I.C. (2010); AIG CyberEdge Security and Privacy Liability Insurance,

endorsements to traditional policies that may extend various coverages to cyber risks,[13] though those endorsements are often narrowly drawn.[14] New policy offerings may present opportunities to fill gaps in an existing coverage program; however, these new insurance products should be carefully evaluated to compare the coverage offered to a particular company's cyber risk profile, including its exposure to data and privacy breaches and to insurance already available to it from traditional coverages.

The next section of this chapter discusses some of the issues that have arisen from the application of traditional insurance coverages to cyber losses and privacy breaches. While there is still only limited case law analyzing the newer cyber policies, the chapter then discusses some of the issues to consider with respect to these more recent forms.

§ 16:2 Applicability of Historic Coverages

Where coverage is sought for data privacy or security breaches under traditional policies, the focus is most commonly on CGL and property policies, though other coverages such as directors and officers liability (D&O), errors and omissions (E&O), and crime policies may come into play as well.

§ 16:2.1 First- and Third-Party Coverages for Property Loss

Insurance practitioners typically distinguish between two types of coverage—first-party coverage, which generally insures a loss to the insured's own property; and third-party coverage, which generally

---

Form 101024 (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf.

13. *See, e.g.*, Complaint, Clarus Mktg. Grp., LLC v. Phila. Indem. Ins. Co., No. 11-2931 (S.D. Cal. 2011) (the "Network Security and Privacy Liability Coverage Endorsement" covered damages against "any actual or alleged breach of duty, neglect, act, error or omission that result[s] in a Privacy Breach"; the parties ultimately settled and filed a joint motion to dismiss).

14. *See, e.g.*, Universal Am. Corp. v. Nat'l Union Fire Ins. Co., 38 Misc. 3d 859 (N.Y. Sup. Ct.), *aff'd*, 110 A.D.3d 434 (N.Y. App. Div. 2013), *aff'd*, 25 N.Y.3d 675 (2015) (coverage denied because "Computer Systems Fraud" rider to the insured's Financial Institution Bond was not intended to cover "fraudulent claims which were entered into the system by authorized users"); Tornado Techs., Inc. v. Quality Control Inspection, Inc. 977 N.E.2d 122 (Ohio Ct. App. 2012) (coverage denied because "Computer Coverage Form" did not apply to the location where back-up servers were located.

provides insurance for liability claims asserted against the insured by third parties for bodily injury, personal injury, or damage to the claimant's property.[15]

In the absence of dispositive exclusions for cyber risks, the availability of coverage for privacy breaches or other cyber risks under a first-party property policy or the property liability coverage of a third-party CGL policy usually turns on the issue of whether the loss of computer data or information constitutes "physical damage" to "tangible property" under the governing policy language. Although first-party and third-party coverages apply to different types of losses, the same definitional issues are often raised by cyber claims and analyzed by courts assessing the availability of each kind of insurance. In each case, "property damage" is typically defined in the policy or by case law as "physical injury to tangible property, including resulting loss of use of that property . . . , or loss of use of tangible property that is not physically injured."[16]

Courts are divided as to whether property losses relating to computer software and data constitute "physical injury" to "tangible property" for purposes of an insurance claim. While cases have held repeatedly that physical damage to computer hardware is covered under first- and third-party insurance policies,[17] courts have

---

15. *See, e.g.*, Port Auth. v. Affiliated FM Ins. Co., 245 F. Supp. 2d 563, 577 (D.N.J. 2001) (explaining that third-party "liability insurance, which indemnifies one from liability to third persons, is distinct from first-party coverage, which protects against losses sustained by the insured itself") (citation omitted), *aff'd*, 311 F.3d 226 (3d Cir. 2002). *See generally* ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES §§ 6:5 & 6:6 (6th ed. Updated Online Mar. 2022).

16. *See, e.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 801–02 (8th Cir. 2010) (liability insurance policy defined "property damage" as "physical injury to tangible property, including resulting loss of use of that property . . . or loss of use of tangible property that is not physically injured"); Big Constr., Inc. v. Gemini Ins. Co., 2012 WL 1858723, at *8 (W.D. Wash. May 22, 2012) (policy defined "property damage" as "[p]hysical injury to tangible property, including all resulting loss of use of that property" and "[l]oss of use of tangible property that is not physically injured"); Auto-Owners Ins. Co. v. Pozzi Window Co., 984 So. 2d 1241, 1244 (Fla. 2008) (same); Mangerchine v. Reaves, 63 So. 3d 1049, 1055 n.5 (La. Ct. App. 2011) (in first-party claim against insurer, policy defined "property damage" as "physical injury to, destruction of, or loss of use of tangible property"). *See generally* ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 11:1 (6th ed. Updated Online Mar. 2022).

17. *E.g.*, Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W.3d 16, 23–25 (Tex. App. 2003) (holding that first-party policy covered data losses due to damage to computer server: "the server falls within the definition of 'electronic media and records' because it contains a hard drive

sometimes struggled with the issue of whether damage to data or software alone qualifies as physical injury to tangible property.[18]

[A] First-Party Property Policies

Cases are divided over whether loss or damage to data or software is covered under traditional first-party property policies.[19] While some courts have taken the position that software and data are not tangible property,[20] others have applied a broader definition

---

or 'disc' which could no longer be used for 'electronic data processing, recording, or storage'"); Nationwide Ins. Co. v. Hentz, 2012 U.S. Dist. LEXIS 29181 (S.D. Ill. Mar. 6, 2012), *aff'd*, Nationwide Ins. Co. v. Cent. Laborers' Pension Fund, 704 F.3d 522 (7th Cir. 2013) (finding "property damage" under homeowner's insurance policy since the insured's losses resulted from the theft of a CD-ROM, which constituted "tangible property"; however, an exclusion still applied to bar coverage); Cincinnati Ins. Co. v. Prof'l Data Servs., Inc., 2003 WL 22102138, at *5–8 (D. Kan. July 18, 2003) (for purposes of third-party coverage; damage to computer hardware constitutes "property damage" and would trigger coverage, but damage to software alone does not).

18. *See infra* section 16:2.1[A]–[B].

19. The numerous recent cases relating to insurance for business interruption due to the COVID-19 pandemic emphasize the importance, and explore the meaning, of the concepts of "physical damage" and "loss of use" under first party policies and may be cited in the cyber context; however, the decisions, which continue to evolve, often turn on allegations and factual circumstances specific to the COVID pandemic rather than the science of cyber technology and therefore are not discussed here. *See generally* Daphne Zhang, *Covid Insurance State Court Rulings Reflect 'Long Game' Ahead*, BLOOMBERG LAW (June 21, 2022), https://news.bloomberglaw.com/insurance/covid-insurance-state-court-rulings-reflect-long-game-ahead; Steven R. Gilford & Charles Gordon, *How the UK and US are dealing with COVID-19-related insurance claims*, WESTLAW TODAY (Aug. 16, 2021), today.westlaw.com/Document/I06cc0c96feab11ebbea4f0dc9fb69570/View/FullText.html; *Covid Coverage Litigation Tracker*, Univ. of Penn. Carey Law Sch. (last visited Aug. 10, 2022), https://cclt.law.upenn.edu/.

20. *See, e.g.*, Metro Brokers, Inc. v. Transp. Ins. Co., 603 F. App'x 833 (11th Cir. 2015) (holding that the insured's first-party property policy's coverage of "forgery" applied only to so-called traditional negotiable instruments and, therefore, there was no coverage for the fraudulent electronic transfer of money from the insured's client's escrow accounts); Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., 2016 U.S. Dist. LEXIS 147361 (N.D. Ala. Oct. 25, 2016) (claims related to compromised electronic data were not claims for property damage); Liberty Corp. Capital Ltd. v. Sec. Safe Outlet, Inc., 937 F. Supp. 2d 891, 901 (E.D. Ky. 2013) (email addresses stolen from electronic databases did not constitute "tangible property" and were excluded by policy's exclusion of "electronic data"); Carlon Co. v. Delaget, LLC, No. 11-CV-477-JPS, 2012 WL 1854146 (W.D. Wis.

of "physical damage" and held that data itself constitutes physical property.[21] In addition, various cases have held that the inability to use a computer due to damaged data may constitute "loss of use" and thus covered property damage under a first-party policy,[22] at least

---

May 21, 2012) (holding electronic funds were not tangible property); Greco & Traficante v. Fid. & Guar. Ins. Co., 2009 Cal. App. Unpub. LEXIS 636, at *12–13 (Ct. App. Jan. 26, 2009) (data lost due to power outage that did not damage physical media such as disks or computers not covered by a first-party property policy); Ward Gen. Servs., Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844 (Ct. App. 2003) (data loss due to a computer crash and human error did not constitute a loss of tangible property under a first-party policy).

21. *See, e.g.*, NMS Servs., Inc. v. Hartford, 62 F. App'x 511, 515 (4th Cir. 2003) (concurring opinion) (data erased by a hacker was "direct physical loss"); Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc., 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 26, 2012) (electronic data, while not tangible, is physical, and therefore susceptible to "direct, physical 'loss or damage'"); Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831 (W.D. Tenn. 2006) (first-party property policy covered loss of use of a computer as "property damage" after loss of stored programming information and configurations); Am. Guar. & Liab. Ins. Co. v. Ingram Micro, No. 99-185, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (reasoning, based on analysis of state and federal criminal statutes, that loss of data constitutes physical damage under first-party business interruption policy); S. Cent. Bell Tel. Co. v. Barthelemy, 643 So. 2d 1240, 1244 (La. 1994) (electronic software data is physical); Comput. Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.3d 1264, 1266 (N.M. Ct. App. 2002) (computer data is physical, and its loss is covered under third-party policy); Retail Sys. Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 738 (Minn. Ct. App. 1991) (affirming that computer tapes and data were tangible property); Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co., 435 F. Supp. 3d 679, 682–83 (D. Md. 2020) (data and software covered in ransomware attack, finding "loss of use, loss of reliability, or impaired functionality demonstrate the required damage to a computer system consistent with the 'direct physical loss or damage' language in the policy"); EMOI Servs., LLC v. Owners Ins. Co., 180 N.E.3d 683, 694–96 (Ohio Ct. App. 2021), *appeal allowed sub nom.* 181 N.E.3d 1210 (Ohio 2022) (damage to insured's computer system following a ransomware attack was "physical loss or damage" because the policy covered data and software, and therefore contemplated they could be physically damaged). *See also* Kimmelman v. Wayne Ins. Grp., No. 18 CV 1041 (Ohio Ct. Com. Pl. Sep. 25, 2018) (stolen Bitcoin is "property" under homeowner's policy); *AA v. Persons Unknown [2019] EWHC 2556 (Comm) (bitcoin held to be property under English law)*.

22. *See, e.g.*, Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831, 838 (W.D. Tenn. 2006) ("property damage" includes not only "physical destruction or harm of computer circuitry, but also loss of access, loss of use, and loss of functionality," so a first-party property policy covered

in the absence of an applicable exclusion for wear and tear or latent defect.[23]

While decisions have found coverage for lost or damaged data as property damage under traditional first-party property policies,[24] many insurers have responded by taking steps to exclude electronic data from the definition of tangible property.[25] Indeed, the Insurance

---

loss of use of a computer after loss of stored programming information and configurations); Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W.3d 16, 23–24 (Tex. App. 2003) (loss of use of computers, as well as loss of data, constituted physical loss and fell within the scope of policy coverage); Metalmasters of Minneapolis, Inc. v. Liberty Mut. Ins. Co., 461 N.W.2d 496, 502 (Minn. Ct. App. 1990) (data loss covered by first-party property policy because computer tapes themselves were physically damaged in flood); Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co., 435 F. Supp. 3d 679, 686 (D. Md. 2020) ("physical loss or damage to" policy language did not require the computer system's "utter inability to function" and provided coverage for "loss of use, loss of reliability, or impaired functionality"); *EMOI Servs.*, 180 N.E.3d at 694–96 (damage to insured's computer system was "physical loss or damage" because the policy covered the insured's servers, which were inaccessible following the ransomware attack).

23. *See, e.g.*, GF&C Holding Co. v. Hartford Cas. Ins. Co., No. 11-cv-00236, 2013 U.S. Dist. LEXIS 38669, at *9–10 (D. Idaho Mar. 15, 2013) (finding property damage where insured's hard drives failed, but holding coverage unavailable where exclusion provided that insurer "will not pay for physical loss or physical damage caused by or resulting from . . . wear and tear . . . [or] latent defect").

24. *See supra* notes 20 and 21.

25. *See, e.g.*, Liberty Corp. Capital Ltd. v. Sec. Safe Outlet, Inc., 937 F. Supp. 2d 891, 901 (E.D. Ky. 2013) (no coverage for misappropriation of email addresses from electronic databases based on finding that customer email list does not fall within definition of "tangible property" and also excluded under electronic data exclusion); RVST Holdings, LLC v. Main St. Am. Assurance Co., 136 A.D.3d 1196, 1198 (N.Y. App. Div. 2016) (denying coverage for third-party claim arising out of data breach, reasoning that the policy provided that "electronic data is not tangible property" and excluded "[d]amages arising out of the loss of . . . electronic data"); Recall Total Info. Mgmt. v. Fed. Ins. Co., No. X07CV095031734S, 2012 Conn. Super. LEXIS 227 (Super. Ct. Jan. 17, 2012), *aff'd*, 83 A.3d 664 (Conn. App. Ct. 2014), *aff'd*, 115 A.3d 458 (Conn. 2015) (because electronic data was specifically excluded, coverage did not exist under CGL and umbrella policies for notification and other costs incurred when unencrypted data tapes containing personal information fell from the back of a truck and were stolen; court found that damage arose from the data, not the actual tapes); Ins. Servs. Office, Inc., Commercial Liability Umbrella Form 00 01 12 04 § V(18)(b) (2004), *available at* LEXIS, ISO Policy Forms ("For the purposes of this insurance, electronic data is not tangible property."). *See generally* 3 MARTHA A. KERSEY, NEW APPLEMAN

Services Office (ISO) amended the definition of property damage in CGL policies in 2001 to specifically omit coverage for "electronic data"[26] and, in 2004, added an exclusion for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[27] While some policies utilize such an exclusion,[28] others provide coverage for such losses and related business interruption.[29] Boiler and machinery policy forms and endorsements may also provide cyber coverage for certain mechanical or electrical failures.[30]

[B] Third-Party CGL Policies: Coverage for Property Damage Claims

Courts have been similarly mixed in deciding whether lost data or software constitute covered property damage in the context of third-party CGL policies. In some cases, the courts have found that

---

ON INSURANCE LAW LIBRARY EDITION § 18.02[4][a] (2020) (standard CGL policy form now defines electronic data and specifically excludes it from the definition of property damage).

26. *See, e.g.*, Jeff Woodward, *The 2001 ISO CGL Revision*, INT'L RISK MGMT. INST., INC. (Jan. 2002), www.irmi.com/articles/expert-commentary/the-2001-iso-cgl-revision; *see also* Ellicott City Cable, LLC v. Axis Ins. Co., 2016 U.S. Dist. LEXIS 95819 (D. Md. July 22, 2016) (policy excluding "intentional unauthorized access of 'data or systems,'" though television programming was not data).

27. *See, e.g.*, Jeff Woodward, *The 2004 ISO CGL Policy*, INT'L RISK MGMT. INST., INC. (Apr. 2004), www.irmi.com/articles/expert-commentary/the-2004-iso-cgl-policy.

28. *See, e.g.*, Greco & Traficante v. Fid. & Guar. Ins. Co., 2009 Cal. App. Unpub. LEXIS 636, at *12–13 (Ct. App. Jan. 26, 2009) (because computer and disks were not damaged, data loss was not covered by a first-party property policy). Moreover, in some traditional first-party property policies, where data is specifically covered, the sublimit is often low and the value of lost data is limited to the cost of blank media if the data is not replaced. *See, e.g.*, Chubb "Electronic Data Processing Property" coverage form (80-02-1017 (Rev. 7-03)) (coverage for "electronic data" subject to sublimit and valuation based on replacement or reproduction cost, but if data is not replaced or reproduced, coverage is limited to cost of blank media).

29. The FM Global "Advantage" policy is marketed to cover damage to data and software, computer network service interruption, cloud outage, and resulting property damage and business interruption. *See* www.fmglobal.com/products-and-services/products/cyber-resilience-solutions.

30. Navetta, Jacques & Moura, *Boiler and Machinery Insurance Can Boost Cyber Coverage*, LAW360 (Mar. 31, 2021), www.law360.com/articles/1370574/boiler-and-machinery-insurance-can-boost-cyber-coverage.

liability based on loss of data does not trigger coverage.[31] For example, in *America Online, Inc. v. St. Paul Mercury Insurance Co.*,[32] the Fourth Circuit concluded that damage to and loss of use of customers' data and software were not covered under a CGL policy because there was no damage to "tangible property" under the definition of "property damage."[33] The court reasoned that computer data was "an abstract idea in the minds of the programmer and the user," so loss or damage to software or data was "not damage to the hardware, but to the idea."[34]

Other courts have applied a broader concept of "physical damage" and held that data constitutes physical property.[35] For example, in *Computer Corner, Inc. v. Fireman's Fund Insurance Co.*,[36] the court reasoned that because computer data "was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed," the lost data was covered under a CGL policy.[37] In addition, courts have held that an alleged "loss of use" may constitute covered property damage under a CGL policy, where there is appropriate policy wording.[38]

In *Eyeblaster, Inc. v. Federal Insurance Co.*,[39] an Internet advertising company, Eyeblaster, sought coverage under two policies, a general liability policy and an information and network technology errors and omissions liability policy, for claims alleging that its

---

31. *See, e.g.*, Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003) (discussed in following text); State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (reasoning that computer data is not tangible property).
32. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003).
33. *Id*. at 96.
34. *Id*. at 95–96.
35. Comput. Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.3d 1264 (N.M. Ct. App. 2002) (discussed *infra*); *see also* Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010) (discussed in following paragraph of text); NMS Servs., Inc. v. Hartford, 62 F. App'x 511, 515 (4th Cir. 2003) (Widener, J., concurring) (stating that data erased by a hacker was a "direct physical loss").
36. Comput. Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.3d 1264 (N.M. Ct. App. 2002).
37. *Id*. at 1266.
38. *See, e.g.*, State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (computer data was not tangible property, but a computer is tangible property so loss of use of that property constitutes property damage where the policy includes coverage for "loss of use of tangible property").
39. Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010).

products had caused damage to a user's computer.[40] After stating that the plain meaning of "tangible property" includes computers,[41] the Eighth Circuit ruled that the claims against Eyeblaster fell within the CGL policy because the underlying suit repeatedly alleged a "loss of use" of a computer.[42] The court found coverage even though the CGL policy excluded electronic data from the definition of "tangible property."[43] According to the court, the alleged "loss of use" of the physical computer hardware implicated coverage under the policy.[44] Under this approach, though the loss of data itself may not be covered under a traditional CGL policy because it fails to qualify as damage to tangible property, the loss of use of computer hardware due to a loss of data may allow coverage.

Although some decisions find that lost or corrupted data or loss of use constitutes property damage,[45] evolving policy definitions and exclusions in CGL policies now often state specifically that electronic data is not tangible property covered under property damage provisions or exclude damages arising out of the loss of use of electronic data.[46] As a result, policyholders seeking insurance for a data loss under the property damage provisions of a traditional CGL policy may increasingly encounter obstacles to obtaining such coverage. While insureds confronted with a cyber loss should evaluate the availability of coverage under property damage provisions of CGL

---

40. *Id*. at 799.
41. *Id*. at 802.
42. *Id*.
43. *Id*.
44. *Id. See also* Target Corp. v. Ace Amer. Ins. Co., No. 19-CV-2916 (WMW/DTS), 2022 WL 848095, at *3 (D. Minn. Mar. 22, 2022) (CGL policy covers settlement Target paid to banks that reissued customer credit cards following data breach as "loss of use" because "[a]lthough the compromised cards still existed, like the consumer's computer in *Eyeblaster*, they could no longer serve their function").
45. *E.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 802 (8th Cir. 2010); Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831, 838 (W.D. Tenn. 2006); Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185, 2000 U.S. Dist. LEXIS 7299, at *10 (D. Ariz. Apr. 18, 2000).
46. *See, e.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 802 (8th Cir. 2010) (definition of "tangible property" excludes "any software, data or other information that is in electronic form"); Ins. Servs. Office, Inc., Commercial Liability Umbrella Form CU 00 01 12 04 § V(18)(b) (2004), *available at* LEXIS, ISO Policy Forms ("For the purposes of this insurance, electronic data is not tangible property."); Ins. Servs. Office, Inc., Commercial Liability Umbrella Coverage Form CU 00 01 12 04 § A.2.t (2004), *available at* LEXIS, ISO Policy Forms (excluding "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data").

policies, another successful avenue for coverage of data breach and privacy claims—at least in the liability context—is often found in the coverage for personal and advertising injury.[47]

§ 16:2.2 CGL Coverage for Personal and Advertising Injury Claims

CGL policies typically provide liability coverage for damages arising from claims against the insured that involve bodily injury, property damage, advertising injury, and personal injury. While insurers continue to add exclusions in an effort to restrict insurance for cyber claims,[48] in addition to the CGL property damage coverage discussed above,[49] insurance for data breaches and privacy-related claims may exist under CGL policy provisions insuring "personal injury" and "advertising injury," particularly where they include coverage for liability arising from "oral or written publication, in any manner, of material that violates a person's right of privacy."[50]

---

47. *See infra* section 16:2.2.

48. The April 2013 revisions to the ISO CGL form introduced a new endorsement entitled "Amendment of Personal and Advertising Injury Definition." This endorsement explicitly excludes the right of privacy provision from paragraph 14.e. of the Personal and Advertising Injury definitions section ("[o]ral or written publication, in any manner, of material that violates a person's right of privacy"). Ins. Servs. Office, Inc., Commercial Liability Form CG 24 13 04 13 (2013), *available at* LEXIS, ISO Policy Forms; *see also supra* section 16:2.1[B].

49. *See supra* section 16:2.1[B].

50. Two illustrative provisions are as follows:

> "Personal injury" is defined as an injury, other than "bodily injury," arising out of certain enumerated offenses including: 1) false arrest, detention or imprisonment, 2) malicious prosecution, 3) wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies by or on behalf of its owner, landlord or lessor, 4) oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services, or 5) *oral or written publication of material that violates a person's right of privacy*.
>
> 9A STEVEN PLITT ET AL., COUCH ON INSURANCE § 129:8 (3d ed. Updated Online June 2022) (emphasis added).
>
> "Advertising injury" is defined as injury arising out of certain enumerated offenses, including: 1) oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services; 2) *oral or written publication of material that violates a person's right of privacy*; 3) misappropriation of advertising ideas or style of doing business; or 4) infringement of copyright, title, or slogan.

Personal and advertising injury provisions often limit coverage to specifically enumerated offenses like malicious prosecution or copyright infringement.[51] For coverage of data breaches, the most important of these enumerated offenses is usually "oral or written publication, in any manner, of material that violates a person's right of privacy."[52] Some policies and courts limit coverage for violation of a right to privacy to injuries caused by an insured's "advertising" activity,[53] but others include this coverage for any publication.[54]

Id. § 129:9 (emphasis added); *see, e.g.*, Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., No. CCB-06-2055, 2007 U.S. Dist. LEXIS 81570, at *3–4 (D. Md. Oct. 26, 2007). *But see supra* note 48.

51. 9A STEVEN PLITT ET AL., COUCH ON INSURANCE § 129:9 (3d ed. Updated Online June 2022); *see supra* note 48.

52. *See, e.g.*, Ins. Servs. Office, Inc., Commercial General Liability Form CG 00 01 10 01, § V(14)(e) (2008), *available at* LEXIS, ISO Policy Forms; *see also* Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF JCX, 2013 U.S. Dist. LEXIS 152836 (C.D. Cal. Oct. 7, 2013) (holding that a hospital data breach was covered under the CGL policy provision that includes "electronic publication of material that violates a person's right of privacy"). *But see* ISO Form CG 24 13 04 13 (2013) (specifically excluding violation of right to privacy as an enumerated offense), quoted in *supra* note 48.

53. 3 ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 11:29 (6th ed. Updated Online Mar. 2022) ("modern liability policies typically include a distinct coverage part for *advertising injury* caused by an offense committed both during the policy period and in the course of advertising the insured's goods or services") (emphasis added); *see also* Hyundai Motor Am. v. Nat'l Union Fire Ins. Co., 600 F.3d 1092, 1098 (9th Cir. 2010) (holding "advertising" means "widespread promotional activities usually directed to the public at large," but "does *not* encompass 'solicitation'") (citation omitted); Simply Fresh Fruit, Inc. v. Cont'l Ins. Co., 94 F.3d 1219, 1223 (9th Cir. 1996) ("under the policy, the advertising activities must cause the injury—not merely expose it"); Air Eng'g, Inc. v. Indus. Air Power, LLC, 828 N.W.2d 565, 572 (Wis. Ct. App. 2013) (court defined an "advertising idea" as "an idea for calling public attention to a product or business, especially by proclaiming desirable qualities so as to increase sales or patronage"); Lexmark Int'l, Inc. v. Transp. Ins. Co., 327 Ill. App. 3d 128, 137 (App. Ct. 2001) (while there is no generally accepted definition of advertising activity in the context of "personal and advertising injury" insurance coverage, the court found it generally referred to "the widespread distribution of promotional material to the public at large"); Phx. Am., Inc. v. Atl. Mut. Ins. Co., 2001 WL 1649243, at *6 (Cal. Ct. App. Dec. 24, 2001) (unpublished) (court defined "advertising" for purposes of CGL insurance coverage as "the act of calling public attention to one's product through widespread promotional activities").

54. *See, e.g.*, Ins. Servs. Office, Inc., Commercial Gen. Liab. Coverage Form CG 00 01 12 07, § V(14) (2008), *available at* LEXIS, ISO Policy Forms (indicating that both personal injury and advertising injury can arise

Two key issues in seeking insurance for cyber risks under personal or advertising injury clauses of a traditional CGL policy are whether there has been a covered publication of information and whether a third party's right to privacy was implicated.[55]

[A] Publication Requirement

Particularly where advertising is required for coverage, insurers have frequently raised the issue of whether the event implicating coverage constitutes a "publication." The importance of the publication requirement is illustrated by *Recall Total Information Management v. Federal Insurance Co.*,[56] where the insured lost computer tapes containing sensitive information of thousands of its clients' employees. In that case, the court held that there was no publication since the insured could not establish that the information contained on the lost tapes was ever accessed by anyone, which the court found to be a "necessary prerequisite to the communication or disclosure of personal information."[57]

Where there is dissemination, however, the issue becomes how widely that information must be disseminated in order to constitute publication. In *Netscape Communications Corp. v. Federal Insurance Co.*,[58] the underlying complaint alleged that Netscape had intercepted

---

from oral or written publication that violates a person's right to privacy); Am. Family Mut. Ins. Co. v. C.M.A. Mortg., Inc., No. 1:06-cv-1044, 2008 U.S. Dist. LEXIS 30233, at *16 (S.D. Ind. Mar. 31, 2008) (covering "oral or written publication, *in any manner*, of material that violates a person's right of privacy"; the "in any manner" language "le[ft] no room for equivocation" in holding that the insurer had a duty to defend the underlying Fair Credit Report Act violation case based on a solicitation letter, including with respect to statutory damages) (emphasis added); *see also* Evanston Ins. Co. v. Gene by Gene Ltd., 155 F. Supp. 3d 706 (S.D. Tex. 2016) (granting judgment to insured and finding that insurer must provide defense under coverage for advertising injury and personal injury where company allegedly published results of customers' DNA tests without consent, despite allegation that breach violated Genetic Privacy Act).

55. *See infra* section 16:2.2.

56. Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664, 672–73 (Conn. App. Ct. 2014), *aff'd*, 115 A.3d 458 (Conn. 2015). *But see infra* note 63 for cases on both sides of the issue.

57. Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664, 672–73 (Conn. App. Ct. 2014); *see also* Defender Sec. Co. v. First Mercury Ins. Co., 803 F.3d 327 (7th Cir. 2015) (no coverage for alleged secret recording of sales calls because the recording of a phone call, without more, is insufficient to constitute a publication).

58. Netscape Commc'ns Corp. v. Fed. Ins. Co., 343 F. App'x 271 (9th Cir. 2009).

and internally disseminated private online communications.[59] The court held that internal disclosures of computer communications triggered coverage because the policy language covered disclosure to "any" person or organization.[60] Therefore, even though the alleged disclosure was confined within the company, coverage was triggered.[61]

As illustrated by *Netscape*, the publication requirement has often required a rather limited showing by those seeking coverage. While the cases are not uniform on this point,[62] various courts have held that an insured need not disclose information widely or externally to satisfy the requirement of publication in cases involving data breaches or unauthorized disclosure of private information.[63]

---

59. *Id*. at 272.
60. *Id*.
61. *Id*.
62. *See also infra* notes 63–68 and accompanying text.
63. *Compare* Landry's, Inc. v. Ins. Co. of the State of Pennsylvania, 4 F.4th 366 (5th Cir. 2021) (defining publication broadly so that publication of customers' credit card information requires only exposing it to a single other person, therefore finding instances of publication both when the insured "exposed" the information to hackers and when the hackers "exposed" the information to make fraudulent purchases); Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC, 35 F. Supp. 3d 765 (E.D. Va. 2014) (holding that "[p]ublication occurs when information is 'placed before the public,' not when a member of the public reads the information placed before it"), *aff'd*, 644 F. App'x 245 (4th Cir. 2016); Netscape Commc'ns Corp. v. Fed. Ins. Co., 343 F. App'x 271 (9th Cir. 2009) (publication requirement of policy was satisfied where disclosures were internal to the company); Encore Receivable Mgmt., Inc. v. Ace Prop. & Cas. Ins. Co., No. 1:12-cv-297, 2013 U.S. Dist. LEXIS 93513, at *31 n.17 (S.D. Ohio July 3, 2013), *vacated by settlement*, No. 1:12-cv-297, 2014 U.S. Dist. LEXIS 146083 (S.D. Ohio May 19, 2014) (internal transmission of information within a corporation constitutes publication); Norfolk & Dedham Mut. Fire Ins. Co. v. Cleary Consultants, Inc., 958 N.E.2d 853 (Mass. App. Ct. 2011) (finding that insured's alleged transmittal of employee's private information to co-workers constitutes "publication" under CGL policy); Virtual Bus. Enters., LLC v. Md. Cas. Co., 2010 Del. Super. LEXIS 141 (Super. Ct. Apr. 9, 2010) (finding transmittal of letters to handful of former clients constituted "publication"); Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., No. CCB-06-2055, 2007 U.S. Dist. LEXIS 81570, at *14 (D. Md. Oct. 26, 2007) ("Of the circuits to examine 'publication' in the context of an 'advertising injury' provision, the majority have found that the publication need not be to a third party.") (citation omitted); and Tamm v. Hartford Fire Ins. Co., 16 Mass. L. Rep. 535 (Super. Ct. July 10, 2003) (accessing private emails and discussing contents with three people constituted publication for purposes of CGL coverage), *with* OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177, 180 (3d Cir. 2015) ("'publication'

Under some decisions, disclosure to a single person, even the owner of the private information, can satisfy the publication requirement for advertising injury coverage.[64] One court of appeals recently concluded, in the context of customers' credit card information, that publication means to "expose[ ] it to view."[65] Even where a publication

---

requires dissemination to the public"); Creative Hospitality Ventures, Inc. v. E.T. Ltd., Inc., 444 F. App'x 370, 373 (11th Cir. 2011) (issuance of a receipt containing sensitive credit card information to a customer did not constitute publication, because it did not involve "dissemination of information to the general public"); C.L.D. v. Wal-Mart Stores, Inc., 79 F. Supp. 2d 1080, 1082–84 (D. Minn. 1999) (finding disclosure to three people insufficient publicity to warrant a claim for invasion of privacy); Beard v. Akzona, Inc., 517 F. Supp. 128, 133 (E.D. Tenn. 1981) (finding that disclosure to only five persons was not sufficient to constitute publication); and Defendant AMCO Insurance Company's Rule 12(b)(6) Motion to Dismiss for Failure to State a Claim, Nat'l Grocers by Vitamin Cottage, Inc. v. Amco Ins. Co., No. 1:16-cv-01326 (D. Colo. Oct. 26, 2016) (insurer argued no information violating a person's privacy rights was published and that the Colorado Supreme Court has held that a publication must involve disclosure of information to the public; case settled with a stipulation to dismiss the case).

64. *See, e.g.*, Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., No. CCB-06-2055, 2007 U.S. Dist. LEXIS 81570, at *17 (D. Md. Oct. 26, 2007) (holding that sending a person's credit report back to that particular person in the form of a prescreened letter for a mortgage constituted publication); Pietras v. Sentry Ins. Co., No. 06 C 3576, 2007 U.S. Dist. LEXIS 16015, at *9–10 (N.D. Ill. Mar. 6, 2007) (publication of a consumer's credit information back to that one particular consumer can constitute publication); Motorist Mut. Ins. Co. v. Dandy-Jim, Inc., 912 N.E.2d 659, 666 (Ohio Ct. App. 2009) (insured's publication need not be made to person other than one whose privacy rights were violated); Hill v. MCI WorldCom Commc'ns, Inc., 141 F. Supp. 2d 1205, 1213 (S.D. Iowa 2001) (communication to one person constituted publicity due to confidential relationship between plaintiff and third party); W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 2021 IL 125978, ¶¶ 39–43 (providing fingerprint data to single vendor constituted publication for purposes of personal injury coverage). *See* section 16:2.2[B][2] for discussion.

65. Landry's, Inc. v. Ins. Co. of the State of Pennsylvania, 4 F.4th 366 (5th Cir. 2021) (broadly defining publication and finding that publication of customers' credit card information when the insured "exposed" the information to hackers and when the hackers "exposed" the information to make fraudulent purchases); Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC, 35 F. Supp. 3d 765 (E.D. Va. 2014) (holding that "[p]ublication occurs when information is 'placed before the public,' not when a member of the public reads the information placed before it"), *aff'd*, 644 F. App'x 245 (4th Cir. 2016). *But see* OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177, 180 (3d Cir. 2015) ("'publication' requires dissemination to the public"); Creative Hospitality Ventures, Inc. v. E.T. Ltd., Inc., 444 F. App'x 370, 373 (11th Cir. 2011)

must be a dissemination to the "public," courts have found coverage in cases involving widely disseminated information, like sending thousands of fax advertisements[66] or posting information to the Internet, regardless of whether there is any evidence that the posting was actually read.[67] Disclosure to a recording device has also been held to constitute publication.[68]

Although the publication requirement has been interpreted to apply to a broad range of potential disclosures,[69] some courts still require a definable disclosure to a party other than the person alleging the unauthorized disclosure.[70] In addition, under some

---

(issuance of a receipt containing sensitive credit card information to a customer did not constitute publication, because it did not involve "dissemination of information to the general public").

66. Penzer v. Transp. Ins. Co., 29 So. 3d 1000 (Fla. 2010) (finding coverage where sending thousands of unsolicited fax advertisements fit the "broad definition of 'publication' because it constitutes a communication of information disseminated to the public and it is 'the act or process of issuing copies . . . for general distribution to the public'"); Valley Forge Ins. Co. v. Swiderski Elecs., Inc., 860 N.E.2d 307 (Ill. 2006) (finding coverage where faxing unsolicited advertisements fit plain and ordinary sense of the word "publication" "both in the general sense of communicating information to the public and in the sense of distributing copies of the advertisements to the public"). *But see* Defender Sec. Co. v. First Mercury Ins. Co., 803 F.3d 327 (7th Cir. 2015) (no coverage for alleged secret recording of sales calls because the recording of a phone call, without more, is insufficient to constitute a publication).

67. *See* Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC, 35 F. Supp. 3d 765 (E.D. Va. 2014) (holding that "[p]ublication occurs when information is 'placed before the public,' not when a member of the public reads the information placed before it"), *aff'd*, 644 F. App'x 245 (4th Cir. 2016); Landry's, Inc. v. Ins. Co. of the State of Pennsylvania, 4 F.4th 366 (5th Cir. 2021) (defining "publication in any manner" of customers' credit card information to include "expos[ing] it to view," and finding instances of publication both when the insured "exposed" the information to hackers and when the hackers "exposed" the information to make fraudulent purchases).

68. *See* Encore Receivable Mgmt., Inc. v. Ace Prop. & Cas. Ins. Co., No. 1:12-cv-297, 2013 U.S. Dist. LEXIS 93513, at *29 (S.D. Ohio July 3, 2013), *vacated by settlement*, No. 1:12-cv-297, 2014 U.S. Dist. LEXIS 146083 (S.D. Ohio May 19, 2014) (finding publication by call center recording of conversation without consent); *see also* Complaint, InterContinental Hotels Grp. Res., Inc. v. Zurich Am. Ins. Co., No. 14-CV-04779-YGR (N.D. Cal. Oct. 27, 2014) (seeking a declaration of coverage for underlying putative class action alleging that the insured recorded customer service calls in violation of California's Invasion of Privacy Act).

69. *See supra* notes 65–66, and *infra* notes 119–122.

70. *See* Creative Hospitality Ventures, Inc. v. E.T. Ltd., Inc., 444 F. App'x 370, 373 (11th Cir. 2011) (issuance of a receipt containing sensitive

authorities, CGL policies only provide coverage for publication of information *by the policyholder* rather than by a third-party hacker.[71]

[B] Right to Privacy As an Enumerated Offense

While the contours of the publication requirement continue to develop, many policies, particularly in recent years, do not include a right to privacy as an enumerated offense or contain exclusions designed to preclude coverage for data breaches.[72] Absent inclusion of infringement of a right to privacy as an enumerated offense, the advertising and personal injury sections of CGL policies may not provide coverage for data theft or breach. Where infringement of a right to privacy is included as an enumerated offense, insurers and insureds have had vigorous disputes with respect to whether these provisions encompass data breaches.

---

credit card information to a customer did not constitute publication, because it did not involve "dissemination of information to the general public"); Whole Enchilada, Inc. v. Travelers Prop. Cas. Co. of Am., 581 F. Supp. 2d 677 (W.D. Pa. 2008) (personal and advertising injury provisions of policy were not triggered by alleged violations of the Fair and Accurate Credit Transactions Act where credit card numbers were printed on sales receipts and handed back to the customers themselves); *see also* Defender Sec. Co. v. First Mercury Ins. Co., 803 F.3d 327 (7th Cir. 2015) (no coverage for alleged secret recording of sales calls because the recording of a phone call, without more, is insufficient to constitute a publication); Yahoo! Inc. v. Nat'l Union Fire Ins. Co., 255 F. Supp. 3d 970 (N.D. Cal. 2017) (finding in favor of the insurer and noting that a privacy violation requires disclosure to a third party or publication, but the text messages in this case were sent only to underlying plaintiffs and not third parties), *question certified to California Supreme Court by* 913 F.3d 923 (9th Cir. 2019) (Do unsolicited text messages that do not reveal any private information violate a person's right to privacy?).

71. *See* St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., 337 F. Supp. 3d 1176 (M.D. Fla. 2018) (because the Rosen Hotels' injuries resulted from "the actions of third parties," the claim was not covered under the CGL policies); Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1348 (M.D. Fla. 2017) (finding that "the only plausible interpretation" of the policy language is that the policyholder itself must be accused of publishing the sensitive data); Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (Sup. Ct. Feb. 21, 2014) (disclosure must be by policyholder) (appeal settled without ruling).

72. *See, e.g.*, ISO Endorsement CG 21 07 05 14 (2013) (excluding violation of right to privacy as an enumerated offense), quoted in *supra* note 11; Business Liability Coverage Form BP 0100 01 04, Additional Exclusions § 2 (2004), IRMI.com, www.irmi.com/online/frmcpi/sc0000bp/chaaisbp/01000104.pdf (excludes from coverage any direct or indirect loss or loss of use caused by a computer virus or computer hacking).

In general, courts have explained that the right to privacy contains two distinct rights—the right to seclusion and the right to secrecy.[73] Some courts have used this distinction to conclude that only claims associated with a right to secrecy are insured under policy provisions covering personal and advertising injury.[74] However, others find that any ambiguity associated with the concept of a "right to privacy" in CGL coverage is reason to apply a broad definition covering both types of violations.[75]

---

73. *See, e.g.*, Pietras v. Sentry Ins. Co., 2007 U.S. Dist. LEXIS 16015, at *7–8 (N.D. Ill. Mar. 6, 2007) (privacy interests in seclusion and secrecy are both implicated by a "right to privacy"); ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co., 53 Cal. Rptr. 3d 786 (Ct. App. 2007) (CGL policy covers liability for violations of a privacy right of "secrecy" and not a privacy right of seclusion).

74. *See, e.g.*, Res. Bankshares Corp. v. St. Paul Mercury Ins. Co., 407 F.3d 631 (4th Cir. 2005) (fax advertisements implicate a privacy right of seclusion, while CGL policy coverage relates only to "secrecy" privacy); Md. Cas. Co. v. Express Prods., Inc., Nos. 09-cv-0857, 08-cv-02909, 2011 U.S. Dist. LEXIS 108048, at *53 (E.D. Pa. Sept. 22, 2011), *aff'd*, 529 F. App'x 245 (3d Cir. 2013) (concluding the right to secrecy is only right protected under "personal and advertising injury" of the CGL policies); ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co., 53 Cal. Rptr. 3d 786 (Ct. App. 2007) (a CGL policy covers liability for violations of a privacy right of "secrecy" and not a privacy right of seclusion); Auto-Owners Ins. Co. v. Stevens & Ricci Inc., 835 F.3d 388, 408 (3d Cir. 2016) (insurer had no duty to defend or indemnify TCPA violation claims because "the Policy provides coverage only for violations of the privacy interest in secrecy, and thus does not cover violations of a right to seclusion" caused by junk faxes); Yahoo!, Inc. v. Nat'l Union Fire Ins. Co., 255 F. Supp. 3d 970 (N.D. Cal. 2017) (insurer does not owe a duty to defend for violations of seclusion privacy because "[t]he text messages do not violate a person's privacy right of secrecy") *question certified to California Supreme Court by* 913 F.3d 923 (9th Cir. 2019) (Do unsolicited text messages that do not reveal any private information violate a person's right to privacy?); Selective Ins. Co. of Am. v. J. Reckner Assocs., Inc., No. 2:18-CV-04450-JDW, 2020 WL 1531874, at *3 (E.D. Pa. Mar. 31, 2020) (coverage only available for violation of right of secrecy, not seclusion); *see also infra* note 86 and accompanying text.

75. *See* Owners Ins. Co. v. European Auto Works, Inc., 695 F.3d 814, 821 (8th Cir. 2012) ("The policies' reference to violating a 'right of privacy' thus encompasses the intrusion on seclusion caused by a TCPA violation for sending unsolicited fax advertisements[.]"); Park Univ. Enters. v. Am. Cas. Co., 442 F.3d 1239 (10th Cir. 2006) (holding that the dual meaning of the word "privacy" created an ambiguity in the policy and that it was reasonable to construe "privacy" to include the right to seclusion); Pietras v. Sentry Ins. Co., No. 06-C-3576, 2007 U.S. Dist. LEXIS 16015, at *8 (N.D. Ill. Mar. 6, 2007) ("right to privacy" implicates both seclusion and secrecy); Penzer v. Transp. Ins. Co., 29 So. 3d 1000 (Fla. 2010) (plain meaning of "right to privacy" includes any claim for privacy—whether

Three types of cyber insurance claims that have been litigated under the personal and advertising provisions of CGL policies involve violations of the Telephone Consumer Protection Act (TCPA),[76] state statutes governing collection and use of biometric information,[77] and cases under other statutes, such as those relating to dissemination of ZIP codes[78] or credit card information.[79]

[B][1] Telephone Consumer Protection Act Cases

Coverage cases asserting violations of the TCPA often involve the sending of unsolicited fax advertisements to third-party fax machines[80] or unsolicited text messages to cellular phones.[81] In fax

---

involving a right to secrecy or seclusion); State Farm Fire & Cas. Co. v. Kapraun, No. 310564, 2014 Mich. App. LEXIS 1276, at *5 (Ct. App. July 3, 2014) (rejecting insurer's argument that "'right of privacy' should be limited to the context of Michigan tort law and, further, should only encompass a person's right to secrecy").

76. Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. § 227 (2010), discussed in *infra* section 16:2.2[B][1].

77. *See infra* section 16:2.2[B][2] for discussion.

78. *See, e.g.*, OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177 (3d Cir. 2015), discussed *infra* section 16:2.2[B][3].

79. *See, e.g.*, Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., 2007 U.S. Dist. LEXIS 81570 (D. Md. Oct. 26, 2007) (FCRA claims alleged a violation of a "right to privacy" and insurer had a duty to defend under the "personal and advertising injury coverage" of the insured's policy); FedEx Off. & Print Servs., Inc. v. Cont'l Cas. Co., No. CV204799MWFAGRX, 2020 WL 6804455, at *5 (C.D. Cal. Oct. 20, 2020) (E&O insurer had duty to defend class actions alleging that FedEx violated the Fair and Accurate Credit Transactions Act when policyholder's self-service kiosks printed receipts disclosing too many credit card numbers because the process was unique to FedEx's business model and the policy language included "services related" to professional services), discussed *infra* section 16:2.2[B][3].

80. *See, e.g.*, G.M. Sign, Inc. v. St. Paul Fire & Marine Ins. Co., 768 F. App'x 982 (11th Cir. 2019) (intentional sending of unsolicited fax advertisements under mistaken belief of recipients' prior consent did not constitute an "accident" as required by the CGL policy); Acuity, A Mut. Ins. Co. v. Siding & Insulation Co., 62 N.E.3d 937, 943 (Ohio Ct. App. 8th Dist. 2016) (finding no coverage for unsolicited fax advertisements because a property policy excluded damage that was expected or intended by the insured and thus not caused by an occurrence); Selective Ins. Co. of Am. v. J. Reckner Assocs., Inc., No. 2:18-CV-04450-JDW, 2020 WL 1531874, at *2 (E.D. Pa. Mar. 31, 2020) (no coverage because wear and tear to fax machines was to be expected and the policy excluded coverage for intentional acts); Mesa Labs., Inc. v. Fed. Ins. Co., 436 F. Supp. 3d 1092, 1097 (N.D. Ill. 2020) (same), *aff'd*, 994 F.3d 865 (7th Cir. 2021).

81. *See, e.g.*, Ill. Union Ins. Co. v. U.S. Bus Charter & Limo Inc., 291 F. Supp. 3d 286 (E.D.N.Y. 2018) (violation of TCPA by sending text messages

blast cases, the distinction between the right to seclusion and the right to secrecy has been used to deny coverage where there was found to be a violation of one's right to seclusion, but not of the right to secrecy.[82] Under the cases where the right to seclusion is violated by way of unsolicited faxes or text messages, but there is no accompanying violation of one's interest in the secrecy of personal information, some courts have held there has been no violation of the right to privacy for insurance policy purposes.[83] Other courts have stated that the term "privacy" is ambiguous and can be read to include both a right to secrecy and a right to seclusion.[84]

In light of the decisions upholding personal injury coverage for TCPA claims based on asserted violations of a right of privacy, some

---

advertising bus services covered under professional liability insurance policy); L.A. Lakers, Inc. v. Fed. Ins. Co., 869 F.3d 795 (9th Cir. 2017) (holding invasion of privacy exclusion applied to bar coverage stemming from sending unsolicited text messages); Nat'l Union Fire Ins. Co. v. Papa John's Int'l, Inc., 29 F. Supp. 3d 961 (W.D. Ky. 2014) (finding no coverage for unsolicited text messages sent in violation of the TCPA); Doctors Direct Ins., Inc. v. Bochenek, 38 N.E.3d 116 (Ill. App. Ct. 2015) (holding no coverage for class action involving text messages under cyber claims endorsement of professional liability policy because claims not based on a privacy wrongful act); *see also* Press Release, Fed. Commc'ns Comm'n, FCC Strengthens Consumer Protections Against Unwanted Calls and Texts (June 18, 2015), http://apps.fcc.gov/edocs_public/attachmatch/DOC-333993A1.pdf (announcing increased protection under the TCPA against unwanted robocalls and spam texts). For a discussion of coverage under professional liability errors and omissions policies, *see infra* section 16:2.3[B].

82. *See* Cynosure, Inc. v. St. Paul Fire & Marine Ins. Co., 645 F.3d 1 (1st Cir. 2011) (holding that the policy referred unambiguously to "disclosure" of private third-party information, and not to "intrusion"; therefore the policy did not cover claims for the mere receipt of faxes); Res. Bankshares Corp. v. St. Paul Mercury Ins. Co., 407 F.3d 631 (4th Cir. 2005) (finding that fax advertisements implicate a privacy right of seclusion, while CGL policy coverage relates only to "secrecy" privacy); ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co., 53 Cal. Rptr. 3d 786 (Ct. App. 2007) (holding that advertising injury provisions of a CGL policy did not cover ACS's liability for sending unsolicited fax advertisements because the policy covered only privacy right of "secrecy" and not a privacy right of seclusion); Selective Ins. Co. of Am. v. J. Reckner Assocs., Inc., No. 2:18-CV-04450-JDW, 2020 WL 1531874, at *2 (E.D. Pa. Mar. 31, 2020) (same); *see also supra* 74–75 and accompanying text.

83. *See supra* notes 74–75 and accompanying text; *see also* L.A. Lakers, Inc. v. Fed. Ins. Co., No. CV 14-7743 DMG (SHx), 2015 U.S. Dist. LEXIS 62159 (Apr. 17, 2015), *aff'd*, 869 F.3d 795 (9th Cir. 2017); Doctors Direct Ins., Inc. v. Bochenek, 38 N.E.3d 116 (Ill. App. Ct. 2015).

84. *See supra* note 73.

policies explicitly exclude unsolicited communications,[85] actions for invasion of privacy,[86] and claims for violations of certain statutory actions.[87] Even here, courts have come to different conclusions as to

85. *See, e.g.*, Phx. Ins. Co. v. Heska Corp., No. 15-CV-2435-MSK-KMT, 2017 WL 3190380, at *4 (D. Colo. July 26, 2017) (unsolicited-communications exclusion precluding coverage for damages "arising out of any actual or alleged violation of any law that restricts or prohibits the sending, transmitting or distributing of 'unsolicited communication'").

86. *See, e.g.*, L.A. Lakers, Inc. v. Fed. Ins. Co., 869 F.3d 795, 806 (9th Cir. 2017) (holding that "[b]ecause a TCPA claim is inherently an invasion of privacy claim, [the insurer] correctly concluded that [the claimant]'s TCPA claims fell under the Policy's broad exclusionary clause."); Horn v. Liberty Ins. Underwriters, Inc., 998 F.3d 1289, 1294–95 (11th Cir. 2021) (holding that TCPA class action arose out of an "invasion of privacy," which was specifically excluded by the policy, because the "class complaint specifically alleged that [the insured] invaded the class members' privacy and sought recovery for those invasions").

87. Commercial General Liability Form CG 00 01 12 07, Section I, Coverage B § (2)(P) (2008), *available at* LEXIS, ISO Policy Forms (excludes from coverage "Distribution of Materials in Violation of Statutes"). In November 2013, ISO made available a new endorsement entitled "Access or Disclosure of Confidential or Personal Information and Data Related Liability—with Limited Bodily Injury Exception." Ins. Servs. Office, Inc., Commercial General Liability Form CG 21 07 05 14 (2013), *available at* LEXIS, ISO policy forms (excluding coverage for "damages arising out of: (1) any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information; (2) or loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"); *see also* Nat'l Union Fire Ins. Co. v. Coinstar, Inc., No. C13-1014-JCC, 2014 U.S. Dist. LEXIS 31441, at *5 (W.D. Wash. Feb. 28, 2014) (policy contained an exclusion relating to the violation of statutes banning the sending, transmitting, or communicating any material or information); Nationwide Mut. Ins. Co. v. Harris Med. Assocs., LLC, 973 F. Supp. 2d 1045, 1050 (E.D. Mo. Sept. 23, 2013) (insurance policy contained a Violation of Consumer Protection Statutes exclusion for "'any action or omission that violates or is alleged to violate' the TCPA, or any 'statute . . . that addresses, prohibits or limits the electronic printing, dissemination, disposal, sending, transmitting, communicating or distribution of material or information'"); G.M. Sign, Inc. v. State Farm Fire & Cas. Co., 18 N.E.3d 70, 74 (Ill. Ct. App. 2014), *appeal denied*, 23 N.E.3d 1200 (2015) ("Distribution of Material in Violation of Statutes Exclusion" applied to "Bodily injury, property damage, personal injury, or advertising injury *arising directly or indirectly out of* any action or omission that violates or is alleged to violate [t]he Telephone Consumer Protection Act (TCPA)."") (emphasis added); Am. Econ. Ins. Co. v. Hartford Fire Ins. Co., 695 F. App'x 194 (9th Cir. 2017)

whether exclusions related to the violation of various statutes actually apply to bar coverage, with some courts applying these exclusions,[88] while others have not.[89] In cases where statutory exclusions have

---

(excluding losses arising "directly or indirectly out of any act or omission that allegedly violated any statute that prohibits or otherwise governs the distribution or transmission of material"); Zurich Am. Ins. Co. v. Ocwen Fin. Corp., 990 F.3d 1073, 1076–79 (7th Cir. 2021) (coverage for statutory privacy (TCPA) and credit defamation (FDCPA) counts precluded by CGL policy's exclusions for "Recording and Distribution of Material or Information in Violation of Law" and "Violation of Communication or Information Law" because these counts each arose from TCPA; common law privacy claims also dismissed because each arose out of alleged statutory violations); Mesa Labs., Inc. v. Fed. Ins. Co., 436 F. Supp. 3d 1092, 1097–98 (N.D. Ill. 2020) (relying on two exclusions to bar coverage for TCPA and common law claims for sending unsolicited faxes: (1) intended or expected acts exclusion and (2) information exclusion barring coverage for TCPA violations), *aff'd*, 994 F.3d 865 (7th Cir. 2021).

88. Flores v. ACE Am. Ins. Co., No. 17-cv-8674, 2018 U.S. Dist. LEXIS 73629, at *5 (S.D.N.Y. Apr. 30, 2018) (motion to dismiss in favor of insurer because suit falls under TCPA and consumer protection laws exclusions); Scottsdale Ins. Co. v. Stergo, No. 13 C 5015, 2015 U.S. Dist. LEXIS 127268 (N.D. Ill. Sept. 23, 2015) (exclusion for "violation of statutes that govern emails, fax, phone calls or other methods of sending material or information" barred coverage for sending unsolicited junk fax advertisements); Nat'l Union Fire Ins. Co. v. Coinstar, Inc., 2014 U.S. Dist. LEXIS 31441, at *4 ("Violation of Statutes in Connection with Sending, Transmitting, or Communicating Any Material Or Information" exclusion applied to bar coverage where the plaintiffs alleged a violation of the Video Protection Privacy Act); Regent Ins. Co. v. Integrated Pain Mgmt., S.C., No. 4:14-CV-1759, 2016 WL 6330386, at *7 (E.D. Mo. Oct. 27, 2016) (granting summary judgment in favor of insurers, finding "application of the TCPA exclusion would exclude all of the claims in the Underlying Lawsuit") (applying Illinois law); James River Ins. Co. v. Med Waste Mgmt., LLC, 46 F. Supp. 3d 1350, 1358 (S.D. Fla. 2014) (policy's TCPA exclusion precludes coverage and insurer owes no duty to defend or indemnify for the TCPA claims in the underlying lawsuit); Certain Underwriters at Lloyd's, London v. Convergys Corp., No. 12 Civ. 08968, 2014 WL 376550, at *3 (S.D.N.Y. Mar. 25, 2014) (exclusion bars coverage for claims arising out of violations of consumer protection laws); and Mesa Labs., Inc. v. Fed. Ins. Co., 436 F. Supp. 3d 1092, 1097–99 (N.D. Ill. 2020) (information exclusion applies to TCPA claim and to common law claims where insured's conduct alleged in each count was inexorably intertwined), *aff'd*, 994 F.3d 865 (7th Cir. 2021). *See also infra* notes 99–100 discussing application of exclusions in BIPA cases.

89. Evanston Ins. Co. v. Gene by Gene Ltd., 155 F. Supp. 3d 706, 709 (S.D. Tex. 2016) (policy excluded violations of TCPA, CAN-SPAM, and any other statute that "prohibits or limits the sending, transmitting, communication or distribution of information or other material," but it did

been held to bar insurance for statutory claims, courts are divided on whether to allow coverage for causes of action that would exist in the absence of the relevant statute.[90] In addition, courts are divided on whether TCPA damages are punitive and, therefore, uninsurable as a matter of public policy.[91]

---

not apply to bar coverage of Alaska Genetic Privacy Act claims); Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF (JCx), 2013 U.S. Dist. LEXIS 152836, at *6 (C.D. Cal. Oct. 7, 2013) (the statutory exclusion for "Personal And Advertising Injury . . . [a]rising out of the violation of a person's right to privacy created by any state or federal act" did not apply to bar coverage for the insured hospital's data breach because at common law, medical records have long been deemed confidential and private, and because the legislative history of the relevant statutes shows that they were not enacted to create new privacy rights); W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 2021 IL 125978, ¶¶ 52–60 (violation of statutes exclusion does not apply to BIPA), discussed *infra* at section 16:2.2[B][3].

90. *Compare* Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF (JCx), 2013 U.S. Dist. LEXIS 152836, at *11 (C.D. Cal. Oct. 7, 2013) (statutory exclusion would not apply to damages that would have applied in the absence of the statutes); Nationwide Mut. Ins. Co. v. Harris Med. Assocs., LLC, 973 F. Supp. 2d 1045 (E.D. Mo. 2013) (holding that the Violation of Statutes exclusion did not negate the potential for coverage for common law claims); and Axiom Ins. Managers, LLC v. Capitol Specialty Ins. Corp., 876 F. Supp. 2d 1005, 1015 (N.D. Ill. 2012) (holding that the Distribution of Material exclusion did not exclude coverage of common law claim), *with* Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 957 F. Supp. 2d 1135, 1155–56 (C.D. Cal. 2013), *aff'd*, 635 F. App'x 351 (9th Cir. 2015) (holding that common law claims that were not separate from statutory violations were subject to the statutory exclusions); CE Design Ltd. v. Cont'l Cas. Co., No. 2-15-0530, 2016 WL 2342858 (Ill. App. Ct. May 2, 2016), *appeal denied*, 60 N.E.3d 871 (Ill. 2016) (holding no coverage for common law claims because they arose from the same conduct that was the basis for the TCPA claim); Ill. Cas. Co. v. W. Dundee China Palace Rest., Inc., 49 N.E.3d 420 (Ill. App. Ct. 2015), *appeal denied*, 48 N.E.3d 672 (Ill. 2016) (holding there was no coverage because common law claims were merely a "rephrasing" of the TCPA conduct); and Zurich Am. Ins. Co. v. Ocwen Fin. Corp., 990 F.3d 1073 (7th Cir. 2021) (common law claims dismissed because each arose out of alleged statutory violations of TCPA and Fair Debt Collection Practices Act).

91. *Compare* Ace Am. Ins. Co. v. Dish Network, LLC, 883 F.3d 881, 888 (10th Cir. 2018) ("TCPA's statutory damages are penal under Colorado law and, even if they were otherwise covered under the policies, Colorado's public policy prohibits the insurability of such penalties and bars coverage."), *with* Standard Mut. Ins. Co. v. Lay, 989 N.E.2d 591, 599–600 (Ill. 2013) (court held that TCPA damages of $500 per violation

[B][2] Biometric Information Cases

Increasingly, states are regulating by statute the collection and management of biometric information such as fingerprints, voiceprints, and facial or retina scans.[92] The Illinois Biometric Information Privacy Act (BIPA), which regulates collection, retention, disclosure, and destruction of a person's biometric identifiers,[93] is particularly important from an insurance perspective because it explicitly includes a private right of action for any person "aggrieved" by a violation of the statute.[94] The Illinois Supreme Court has held that plaintiffs can pursue claims without demonstrating "actual damage beyond the violation of his or her rights under the Act."[95] As a result,

---

are not uninsurable punitive damages since the purpose was "clearly" remedial in nature). On remand, the Illinois Appellate Court held that the insurer must provide coverage to the insured for settlement of the underlying TCPA suit. Standard Mut. Ins. Co. v. Lay, 2 N.E.3d 1253 (Ill. App. Ct. 2014), *appeal denied*, No. 117110, 2014 Ill. LEXIS 433 (Mar. 26, 2014). For further discussion of the *Lay* decision, see *infra* section 16:3.2[G]. *See also* Wakefield v. ViSalus, Inc., No. 3:15-cv-1857-SI, 2020 WL 4728878 (D. Ore. 2020) (refusing to reduce as unconstitutionally excessive jury's $925 million verdict—statutory damages of $500 each for 1.85 million violative robocalls); Golan v. FreeEats.com, Inc., 930 F.3d 950 (8th Cir. 2018) ($1.6 billion statutory damages award violated due process and was properly reduced to $32 million—$10 per call that violated TCPA).

92. *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2020); WASH. REV. CODE ANN. § 19.375 (West 2020); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2020). A federal National Biometric Information Privacy Act bill was recently introduced in the U.S. Senate, but the bill did not pass. National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020). The House of Representatives has since introduced a new comprehensive federal privacy law, the American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. (2021–2022). *But see supra* notes 90 and 91.

93. *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2020) (setting out requirements for private entities collecting biometric identifiers: section 15(a) requires entities to develop a publicly available written policy regarding retention and destruction of biometric identifiers; section 15(b) regulates the collection of biometric identifiers; section 15(c) prohibits the sale of biometric information; section 15(d) regulates dissemination or disclosure of the biometric information; and section 15(e) sets the standard of care for such information).

94. 740 ILL. COMP. STAT. ANN. 14/20 (West 2020); *see also* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1204 (Ill. 2019) (private action).

95. *Rosenbach*, 129 N.E.3d at 1205. *See also* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626–27 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* (June 30, 2020) (finding a mere violation of BIPA section 15(b) is sufficient for title III standing, but not section 15(a) as

there have been numerous class actions under this statute,[96] with reported settlements totaling hundreds of millions of dollars.[97]

As the private right of action under BIPA has expanded and the number of filed cases increases, insurers have attempted to limit their potential liability under this type of statute. For example, insurers have invoked, with varying degrees of success, the publication requirement,[98] statutory violations exclusions, and employment practices exclusions,[99] among others, to challenge claims seeking

---

the duty under that section is to the public at large, not a particular individual).

96. *See, e.g.*, Complaint, B.H. v. Amazon.com Inc., No. 2021CH02330 (Ill. Cir. Ct. Cook Cty. May 12, 2021) (alleging that Amazon collected facial data from photos uploaded to the company's photo storage service); First Amended Class Action Complaint, Salkauskaite v. Sephora USA Inc., No. 18-cv-08507 (N.D. Ill. May 7, 2019) (alleging that makeup simulation technology was used to capture customer face scans without permission); Complaint, Barton v. Walmart Inc., No. 2020CH03273 (Ill. Cir. Ct. Cook Cty. July 5, 2021) (alleging Walmart required warehouse workers to use voice recognition software and collected data without workers' consent); Complaint, Barnett v. Apple Inc., No. 2021CH03119 (Ill. Cir. Ct. Cook Cty. June 25, 2021) (alleging Apple's "Touch ID" and "Face ID" features violate Illinois biometric privacy laws by collecting biometric data without consent); Complaint, Svoboda v. Amazon.com Inc., No. 2021CH04516 (Ill. Cir. Ct. Cook Cty. Sept. 7, 2021) (alleging Amazon's "virtual try-on" features on its website and apps breach BIPA because there is no option for Illinois users to opt out of the data collection nor does the company disclose how such data will be retained and eventually destroyed). In more recent cases, plaintiffs have asserted BIPA violations against providers of facial recognition software. *See, e.g.*, Sosa v. Onfido, Inc., No. 20-CV-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022); Gutierrez v. Wemagine.AI LLP, No. 21 C 5702, 2022 WL 252704 (N.D. Ill. Jan. 26, 2022).

97. *See, e.g.*, Lauren Berg, *$650M Facebook Privacy Deal OK'd, $110M Atty Fees Trimmed*, LAW360 (Feb. 26, 2021), www.law360.com/articles/1359569/-650m-facebook-privacy-deal-ok-d-110m-atty-fees-trimmed; Judy Greenwald, *Google agrees to settle biometrics case for $100 million*, BUS. INS. (Apr. 29, 2022), www.businessinsurance.com/article/20220429/NEWS06/912349615/Google-agrees-to-settle-biometrics-case-for-$100-million; Lauren Berg, *TikTok Users Ink $92M Deal To End Biometric Privacy MDL*, LAW360 (Feb. 25, 2021), www.law360.com/articles/1359087; Celeste Bott, *Six Flags Strikes $36M Deal to End Finger Scan Privacy Row*, LAW360 (June 14, 2021), www.law360.com/articles/1393447/six-flags-strikes-36m-deal-to-end-finger-scan-privacy-row.

98. *See, e.g.*, W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 2021 IL 125978, ¶¶ 39–43 (providing fingerprint data to single vendor constituted publication for purposes of personal injury coverage). *See also supra* notes 52 and 53 and accompanying text.

99. *Compare* Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC, No. 20-CV-05980, 2022 WL 602534, at *5 (N.D. Ill. Mar. 1, 2022) (coverage

coverage.[100] Insurers may also argue that statutory damages under

---

was not barred by employment-related practices exclusion because the BIPA claims "do not unambiguously share general similitude with . . . the matters specifically enumerated in the employment-related practices exclusion" nor by statutory or disclosure exclusions); Citizens Ins. Co. of Am. v. Highland Baking Co., Inc., No. 20-CV-04997, 2022 WL 1210709, at *1 (N.D. Ill. Mar. 29, 2022) (same); State Auto. Mut. Ins. Co. v. Tony's Finer Foods Enters., Inc., No. 20-cv-06199, 2022 WL 683688, at *5–9 (N.D. Ill. Mar. 8, 2022) (holding that scanning employees' fingerprints is "categorically different" from the practices listed in the employment practices exclusion); *and* Am. Fam. Mut. Ins. Co., S.I. v. Carnagio Enters., Inc., No. 20 C 3665, 2022 WL 952533, at *6 (N.D. Ill. Mar. 30, 2022) (BIPA claims did not fall within the scope of activities described in the employment-related practices exclusion), *with* Am. Fam. Mut. Ins. Co. v. Caremel, Inc., No. 20 C 637, 2022 WL 79868, at *3–4 (N.D. Ill. Jan. 7, 2022) (holding statutory and disclosure exclusions did not apply, but denying coverage under policy's employment-related practices exclusion because "a BIPA violation is of the same nature as the exemplar employment-related practices listed in the Policy"; Mass. Bay Ins. Co. v. Impact Fulfillment Servs., LLC, No. 1:20CV926, 2021 WL 4392061, at *7 (M.D.N.C. Sept. 24, 2021) (Distribution of Material exclusion applies because BIPA is analogous to TCPA and other statutes concerning "recording" material or information); Nat'l Fire Ins. Co. of Hartford v. Visual Pak, Inc., No. 2020 CH 06897 (Cook Cty. Cir. Ct., Ill. July 7, 2022) at 13 (no duty to defend because Recording and Distribution of Material or Information in Violation of Law Exclusion precluded coverage for statutes that "govern the collection and dissemination of certain information, which BIPA does"); Church Mut. Ins. Co. v. Prairie Vill. Supportive Living, LLC, No. 21 C 3752, 2022 WL 3290686 (N.D. Ill. Aug. 11, 2022) (Violation of Laws Applicable to Employers exclusion precluded coverage under EPL policy); Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc., No. 21 C 788, 2022 WL 954603, at *4–5 (N.D. Ill. Mar. 30, 2022) ("Access Or Disclosure Of Confidential Or Personal Information" exclusion was not ambiguous and precluded coverage for BIPA claims). In one recent case, the court found BIPA liability covered under an Employment Practices Liability policy, but precluded under the insured's D&O policy due to the employment exclusion. Twin City Fire Ins. Co. v. Vonachen Servs., Inc., 567 F. Supp. 3d 979, 999–1002 (C.D. Ill. 2021).

100. *See, e.g.*, Am. Family Mut. Ins. Co. v. Amore Enters., Inc., 2020 WL 1144721 (N.D. Ill. 2020) (complaint) (seeking declaration of no coverage in class action because (1) the policy contains a violation of statute exclusion and an "access to or disclosure of personal information" exclusion; and (2) the policy does not cover claims for "bodily injury" or "personal advertising injury" arising out of employment-related practices); Complaint, Am. Guar. Liab. & Ins. Co. v. Toms King LLC, case number 2020CH04472 (Cir. Ct. Cook Cty. June 5, 2020) (seeking a declaration of no coverage under the policy citing (1) a "Knowing Violation of Rights of Another" exclusion; (2) an "access to or disclosure of personal

BIPA section 15(a) are uninsurable penalties rather than remedial damages.[101]

In the first coverage decision concerning BIPA to reach the Supreme Court of Illinois, the court affirmed a summary judgment in favor of the policyholder on the insurers' duty to defend.[102] In *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*,[103] the insured was sued for unauthorized collection and disclosure of fingerprint data to a third-party vendor in connection with membership to the L.A. Tan national database. The trial and appellate courts rejected the insurer's two grounds for denial—that disclosure to a single vendor did not constitute "publication" under the personal injury coverage and that the "violation of statutes" exclusion applied.[104] Because the policy did not include a definition of "publication," the court relied on dictionary definitions that included both a broad public sharing of information and more limited sharing with a single third party.[105] The court also concluded that the BIPA statute "protects a secrecy interest."[106] In addition, coverage was not barred by an exclusion for violation of TCPA "and other statutes that govern e-mails, fax phone calls or other methods of sending material or information," because that exclusion was meant to bar coverage for a limited type of statute governing the "*methods* of communication" and not statutes limiting the sending or sharing of information.[107] According to the court, "regulating telephone calls, faxes, and e-mails is fundamentally different from regulating the collection, use, storage, and retention of biometric identifiers and information (fingerprints, retina or iris scans, voiceprints, or scans of hand or face geometry)."[108]

---

information" exclusion; (3) a violation of statute exclusion; and (4) and employment-related practices exclusion).

See also McDonald v. Symphony Bronzeville Park, LLC, No. 126511, 2022 WL 318649, at *9–10 (Ill. Feb. 3, 2022) (BIPA claims are not preempted by the exclusivity provisions of the Illinois Workers' Compensation Act because the alleged injuries are not the type compensable in a workers' compensation proceeding); *supra* section 16:2.2 discussing advertising and personal injury claims.

101. *See* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626–27 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* (June 30, 2020) (finding that claimants need not show actual injury under BIPA section 15(a)); *see also supra* note 91 and accompanying text.
102. W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 2021 IL 125978.
103. *Id*. at ¶¶ 1–5.
104. *Id*. at ¶¶ 23–26.
105. *Id*. at ¶¶ 37–43.
106. *Id*. at ¶ 8.
107. *Id*. at ¶¶ 43, 55. *See also supra* notes 99–100.
108. *Id*.

[B][3] ZIP Code, Credit Card, and Other Statutes

Additional types of computer privacy litigation have concerned the gathering of ZIP codes and personal information obtained at the time of credit card purchases. A number of states have statutes that arguably relate to these practices, and several consumer class actions have been brought pursuant to these statutes or common law.[109] Claims for insurance coverage under traditional policies that have arisen in these contexts have had mixed results depending on the policies and circumstances at issue.

With respect to the ZIP code cases, for example, in *OneBeacon American Insurance Co. v. Urban Outfitters*[110] the court rejected one of the insured's claims for coverage on the ground that there was no allegation of public dissemination of information and publication required communication to the public at large. A second claim was rejected on the theory that receipt of unsolicited junk mail alleged a violation of the right to seclusion, not secrecy, and was therefore not within the right of privacy covered by the policy.[111] While it found a third claim alleged sufficient dissemination of personal information to satisfy the publication requirement, the court nonetheless held that coverage was precluded by a statutory exclusion against collecting or recording information.[112] A similar exclusion was applied in *Big 5 Sporting Goods Corp. v. Zurich American Insurance Co.*,[113] in

---

109. *See, e.g.*, OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177 (3d Cir. 2015); Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012).

110. *OneBeacon Am. Ins. Co.*, 625 F. App'x 177 at 180 (requiring publication to be to the "public at large"). *But see supra* notes 58–68.

111. *See id*. at 182.

112. *Id*. at 181–82 (citing the "Recording and Distribution of Material or Information in Violation of Law Exclusion," which excluded "'Personal and advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate . . . [any] statute, ordinance or regulation . . . that addresses, prohibits or limits the . . . dissemination, . . . collecting, recording, sending, transmitting, communicating or distribution of material or information.").

113. Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 957 F. Supp. 2d 1135, 1155–56 (C.D. Cal. 2013), *aff'd*, 635 F. App'x 351 (9th Cir. 2015) (applying the distribution of material in violation of statute's exclusion to coverage for "'[p]ersonal and [a]dvertising [i]njury' arising directly or indirectly out of any action or omission that violates or is alleged to violate: [a]ny statute, ordinance or regulation, other than the TCPA or CAN-SPAM Act of 2003, that prohibits or limits the sending, transmitting, communicating or distribution of material or information"). *But see supra* notes 88–90.

which the court also refused to find a common law claim outside the exclusion.[114]

In general, the Fair Credit Reporting Act (FCRA) governs disclosure of certain personal credit information that is asserted to be confidential. In *Zurich American Insurance Co. v. Fieldstone Mortgage Co.*,[115] a mortgage company seeking coverage was alleged to have improperly accessed and used individual credit information, in violation of FCRA, in order to provide "pre-screened" offers of mortgage services.[116] Confronted with the insurer's denial of the resulting claims,[117] the court noted that FCRA was enacted to ensure the protection of privacy rights and held that the insurer had a duty to defend against FCRA claims because they fell under the "personal and advertising injury coverage" of the insured's CGL policy.[118]

Like many cases involving claims for advertising injury coverage, insurance in *Fieldstone Mortgage* turned on whether the FCRA claim alleged a violation of a "right to privacy" and whether there had been publication of the information at issue.[119] In analyzing the scope of the publication requirement to assess coverage, the court explicitly rejected the insurance company's argument that "in order to constitute publication, the information that violates the right to privacy must be divulged to a third party."[120] Finding that a majority of circuits have rejected this argument,[121] the court held that publication need not be to a third party and that unauthorized access and use was all that was necessary to violate a privacy right for coverage purposes.[122]

§ 16:2.3 Other Coverages

While most companies seeking coverage under traditional policy forms assert claims under first-party property or third-party CGL

---

114. *Id.* at 1151 (because the relevant privacy right was not based on common law and created by statute, coverage for the common law claim was barred by the distribution of material exclusion). *But see supra* notes 90 and 91.
115. Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., 2007 U.S. Dist. LEXIS 81570 (D. Md. Oct. 26, 2007).
116. *Id.* at *2.
117. *Id.* at *4.
118. *Id.* at *9, *11.
119. *See supra* section 16:2.2[A].
120. *Zurich Am.*, 2007 U.S. Dist. LEXIS 81570, at *14 (citing Park Univ. Enters. v. Am. Cas. Co., 442 F.3d 1239, 1248–50 (10th Cir. 2006)).
121. *Id.*; *see also supra* notes 63–70.
122. *Zurich Am.*, 2007 U.S. Dist. LEXIS 81570, at *14, *17–18. *But see supra* note 63.

policies, policyholders may also seek coverage for data or privacy breaches or cyber crime under other contracts in their insurance portfolio, including D&O insurance, E&O policies, and Commercial Crime Policies.

[A] Directors and Officers Liability Insurance

D&O insurance is generally designed to cover losses arising from claims made during the policy period that allege wrongs committed by "directors and officers."[123] As such, this type of insurance may sometimes be limited to circumstances where an officer or director is sued directly in connection with a privacy breach—perhaps for lack of supervision or personal involvement in dissemination of confidential information.

Some D&O policies, and similar policies available to not-for-profits or companies that are not publicly traded, also contain "entity" coverage, which provides insurance for certain claims against the entity itself.[124] In many instances, "entity" coverage is limited to securities claims,[125] but this is not always the case.[126] Where entity coverage is broad, it may encompass liabilities for privacy breaches and other cyber risks.

The relevance of D&O coverage with respect to cyber issues has increased significantly as shareholder derivative actions have been filed against officers and directors of a variety of companies, including

---

123. *See, e.g.*, Sphinx Int'l, Inc. v. Nat'l Union Fire Ins. Co., 412 F.3d 1224, 1227–28 (11th Cir. 2005) (policy providing coverage for duly elected directors and officers for loss incurred in their capacity as directors and officers); PLM, Inc. v. Nat'l Union Fire Ins. Co., No. C-85-7126-WWS, 1986 U.S. Dist. LEXIS 17014, at *6–7 (N.D. Cal. Dec. 2, 1986) (policy provided coverage to individual directors and officers for loss incurred in their capacity as directors and officers), *aff'd*, 848 F.2d 1243 (9th Cir. 1988). *See generally* 4 DAN A. BAILEY ET AL., NEW APPLEMAN ON INSURANCE § 26.01 (2020).

124. *See, e.g.*, AIG Private Company D&O Coverage Section, www.aig.com/business/insurance/management-liability/directors-and-officers-liability.

125. *See, e.g.*, D&O Insuring Agreements, IRMI.com, www.irmi.com/online/pli/ch010/11l10e000/a110e010.aspx#jd_entity_securities_coverage_side_c ("the vast majority of D&O policies that provide entity coverage do so *only* as respects securities claims").

126. *See, e.g.*, AIG Executive Liability, Directors, Officers and Private Company Liability Insurance, Form 95727 (Sept. 2007), § 2(cc)(i) (2007), https://eperils.com/app/95727.pdf (providing coverage for claims against the entity for a "Wrongful Act," including "with respect to a Company, any breach of duty, neglect, error, misstatement, misleading statement, omission or act of a Company.").

Target,[127] Wyndham,[128] Home Depot,[129] Wendy's,[130] and LabCorp,[131] as a result of widely reported cyber breaches involving these companies. These lawsuits challenge the level of supervision by board members and claim that they "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner."[132] The various claims against directors and officers for cyber-related matters, and increasing governmental attention to cyber and privacy issues,[133] underscore the importance of D&O coverage and careful board vigilance in relation to data retention, cybersecurity, and relevant insurance coverage.[134] They also emphasize

---

127. *See In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 490 (D. Minn. 2015) (granting motion for class certification).

128. *See* Complaint, Palkon v. Holmes, No. 2:14-cv-01234 (D.N.J. Feb. 25, 2014); *see also* Palkon v. Holmes, 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (finding that board's decision not to bring suit against the company for inadequate data security was not in violation of the business judgment rule, reasoning that the board took adequate steps to familiarize itself with the subject matter of the demand and that it had ample information at its disposal).

129. *In re* Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1321 (N.D. Ga. 2016), *appeal dismissed*, No. 16-17742-DD, 2017 WL 6759075 (11th Cir. Oct. 24, 2017) (dismissing a shareholder derivative complaint that alleged a breach of fiduciary duties due to defendants' failure to "institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a breach").

130. Complaint, Graham v. Peltz, No. 1:16-cv-01153 (S.D. Ohio Dec. 16, 2016) (case dismissed following settlement), *appeal pending,* No. 21-3975 (6th Cir. Oct. 25, 2021).

131. Complaint, Eugenio v. Berberian, No. 2020-0305 (Del. Ch. Apr. 28, 2020).

132. *See* Complaint, Palkon v. Holmes, No. 14-cv-01234 (D.N.J. Feb. 25, 2014); *see also In re* Heartland Payment Sys., Inc. Sec. Litig., No. 09-1043, 2009 WL 4798148, at *2, *8 (D.N.J. Dec. 7, 2009) (dismissing suit where plaintiffs alleged that the defendants falsely represented that the company "place[d] significant emphasis on maintaining a high level of security" and maintained a network that "provide[d] multiple layers of security to isolate [its] databases from unauthorized access").

133. *See, e.g.*, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, U.S. SEC. & EXCH. COMM'N (Mar. 9, 2022), www.sec.gov/news/press-release/2022-39, discussed in *infra* section 16:3.3, discussed in *infra* section 16:3.3.

134. The Wyndham shareholder derivative litigation (*see supra* note 128) serves as a good example of the risks facing directors and officers from a data breach and how boards can proactively protect themselves to avoid liability in the event of a claim. Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (dismissing a shareholder

the importance to policyholders of avoiding overbroad cyber exclusions in D&O policies so that normal D&O exposures such as an alleged failure to disclose or insufficient board oversight are not excluded simply because they may relate to cyber risks or invasion of privacy.[135]

[B] Errors and Omission Policies

E&O policies provide coverage for claims arising out of the rendering of professional services.[136] Such policies may provide insurance for data breaches or privacy-related claims that arise from the "rendering of services" so long as policy definitions and exclusions do not preclude coverage for losses relating to privacy breaches or Internet-related services.[137] E&O policies designed for medical

---

derivative suit alleging the board failed to take adequate steps to investigate a data breach, reasoning that, among other things, (1) the board discussed cyber-attacks at fourteen meetings prior to the shareholder demand letter; (2) the general counsel gave presentations at the board's quarterly meetings regarding the data breaches and general cybersecurity matters; and (3) the board familiarized itself with the subject matter pursuant to an FTC investigation into the company's security practices); *see also* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Version 1.1) (Apr. 2018), www.nist.gov/cyberframework/framework (providing companies with a set of industry standards and best practices for managing their cybersecurity risks).

135. *See also* L.A. Lakers, Inc. v. Fed. Ins. Co., 869 F.3d 795 (9th Cir. 2017) (court denied coverage under directors and officers liability coverage section based on exclusion for claims arising from invasion of privacy); Horn v. Liberty Ins. Underwriters, Inc., 998 F.3d 1289 (11th Cir. 2021); *infra* note 282.

136. *See, e.g.*, Matthew T. Szura & Co. v. Gen. Ins. Co. of Am., 543 F. App'x 538, 540–41, 543 (6th Cir. 2013) (holding that the E&O policy at issue covered "wrongful acts arising out of the performance of professional services for others," but not "intentionally wrongful conduct"); Pac. Ins. Co. v. Burnet Title, Inc., 380 F.3d 1061, 1062 (8th Cir. 2004) ("Pacific issued an Errors and Omissions (E&O) insurance policy . . . which provided coverage for negligent acts, errors, or omissions in the rendering of or failure to render professional services."). *See generally* 4 PAUL S. WHITE & RICHARD L. NEUMEIER, APPLEMAN ON INSURANCE § 25.01 (2020).

137. *See, e.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 804–05 (8th Cir. 2010) (in addition to finding coverage for property damage under a CGL policy, the court found that coverage existed under an E&O policy, stating that the definition of "error" in a technology errors and omissions policy included intentional, non-negligent acts but excludes intentionally wrongful conduct); Ill. Union Ins. Co. v. U.S. Bus Charter & Limo Inc., 291 F. Supp. 3d 286 (E.D.N.Y. 2018) (company's violation of TCPA by sending text messages advertising bus services covered under professional

professionals or health plan fiduciaries often include specific coverages for HIPAA and other privacy exposures, including computer privacy breaches.[138]

Attorney and other malpractice policies may also cover certain risks associated with unintentional release of confidential information or client funds. For example, in *Stark & Knoll Co. L.P.A. v. ProAssurance Casualty Co.*,[139] the court held that the insured law firm may be covered under its malpractice policy when one of its attorneys fell victim to an alleged phishing scam and sent nearly $200,000 of client funds to an offshore account.[140]

---

liability insurance policy); SS&C Tech. Holdings, Inc. v. AIG Specialty Ins. Co., 436 F. Supp. 3d 739, 745 (S.D.N.Y. 2020) (finding exclusion did not preclude coverage for losses incurred as a result of fraudulently induced transfers due to an email "spoofing" scheme because insured did not contractually have authority over client's funds and because term "lost" in exclusion was ambiguous such that funds wired to fraudsters could be termed "stolen" rather than "lost"); FedEx Off. & Print Servs., Inc. v. Cont'l Cas. Co., No. CV204799MWFAGRX, 2020 WL 6804455, at *5 (C.D. Cal. Oct. 20, 2020) (finding E&O insurer had duty to defend class actions alleging that FedEx violated the Fair and Accurate Credit Transactions Act (FACTA) when policyholder's self-service kiosks printed receipts disclosing too many credit card numbers because the process was unique to FedEx's business model and the policy language included "services related" to professional services). *But see* Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., 103 F. Supp. 3d 1297 (D. Utah 2015) (holding there was no duty to defend under the insured's CyberFirst Policy since the policy covered an "error, omission or negligent act" and the underlying lawsuit alleged that the insured intentionally refused to return the plaintiff's customer data); Margulis v. BCS Ins. Co., 23 N.E.3d 472 (Ill. App. Ct. 2014) (holding that automated telephone calls advertising insured's business did not constitute negligent acts, errors or omissions by insured in "rendering services for others" since the insured was not rendering services for the call recipients).

138. *See, e.g.*, Med. Records Assocs., Inc. v. Am. Empire Surplus Lines Ins. Co., 142 F.3d 512, 516 (1st Cir. 1998) (court noted that hospital employees involved in safeguarding personal medical information may have coverage under an E&O policy given the substantial "risks associated with release of records to unauthorized individuals"); Princeton Ins. Co. v. Lahoda, D.C., No. 95-5036, 1996 WL 11353 (E.D. Pa. Jan. 4, 1996) (finding an improper disclosure of confidential patient information was covered by a professional liability insurance policy).

139. Stark & Knoll Co. L.P.A. v. ProAssurance Cas. Co., No. 12 CV 2669, 2013 U.S. Dist. LEXIS 50326 (N.D. Ohio Apr. 8, 2013).

140. *Id*. at *3, *9–23; *see also* Nardella Chong, P.A. v. Medmarc Cas. Ins. Co., 642 F.3d 941 (11th Cir. 2011) (losses due to Nigerian check scam arose from provision of professional services and were covered by attorney's professional liability insurance policy). *But see* Attorneys Liab. Prot. Soc'y, Inc. v. Whittington Law Assocs., PLLC, 961 F. Supp. 2d 367, 375

Law firms and other providers of services have become repeated targets of cyber attacks seeking confidential client information about transactional and other matters.[141] These kinds of matters may give rise to asserted claims for improper protection of client information.[142]

[C] Crime Policies

Crime policies generally provide first-party coverage and insure a policyholder's property against various forms of theft.[143] In some

---

(D.N.H. 2013) (holding that "the plain and unambiguous language" of policy exclusion "for any claim arising from or in connection with any conversion, misappropriation or improper commingling" excludes coverage for misappropriation of funds).

141. Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Jan. 26, 2018), www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (Equifax, one of the country's largest credit bureaus, experienced a data breach that exposed personal data of about 143 million consumers); Xiumei Dong, *Law Firms' Reported Cyberattacks Are 'Tip of the Iceberg*,' LAW360 (Nov. 4, 2020), www.law360.com/cybersecurity-privacy/articles/1326001?utm_source=shared-articles&utm_medium=email&utm_campaign=shared-articles. A study by the English Solicitors Regulation Authority found cyber theft of more than 4 million pounds sterling from U.K. law firms between 2016 and 2019. Irene Madongo, *Law Firms Targeted by Cybercriminals, Legal Body Warns*, LAW360 (Sept. 3, 2020), www.law360.com/articles/1307024/law-firms-targeted-by-cybercriminals-legal-body-warns; AJ Shankar, *Ransomware Attackers Take Aim at Law Firms*, FORBES (Mar. 12, 2021), www.forbes.com/sites/forbestechcouncil/2021/03/12/ransomware-attackers-take-aim-at-law-firms/?sh=24a61a92a13e.

142. Ben Kochman, *Clients Likely to Grill Law Firms After Vendor Data Breaches*, LAW360 (Feb. 26, 2021), www.law360.com/articles/1359148/clients-likely-to-grill-law-firms-after-vendor-data-breaches. *See also infra* note 293.

143. *See, e.g.*, Colony Tire Corp. v. Fed. Ins. Co., 217 F. Supp. 3d 860 (E.D.N.C. 2016) (crime policy triggered when founders and owners of the company embezzled money); Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 480 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018) (finding coverage for medical data services policyholder because the fraudulently induced transfer was a covered computer fraud under its crime policy); Universal Am. Corp. v. Nat'l Union Fire Ins. Co., 37 N.E.3d 78 (N.Y. 2015) (denying coverage under policy's computer fraud section for Medicare fraud scheme perpetrated by employees, reasoning that use of computer to make false entries about medical treatments that were never provided was merely incidental to fraud scheme); Sanderina, LLC v. Great Am. Ins. Co., No. 218CV00772JADDJA, 2019 WL 4307854, at *3–4 (D. Nev. Sept. 11, 2019) (denying coverage under crime policy for losses sustained when a third party posing as the company owner tricked an employee into transferring money to the imposter because

cases, crime policies also provide third-party coverage against an insured's liability for theft, forgery, or certain other crimes injuring a third party.[144] Insureds are increasingly turning to this type of coverage in cases involving theft by transfer of funds caused by a fraudulent email,[145] as some crime insurance policies explicitly or implicitly provide coverage for computer fraud.[146] With regard to computer-fraud coverage, some courts have come to the conclusion that the

---

scheme did not fit policy definitions); G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 88–89 (Ind. 2021) (finding that "fraudulently cause a transfer" language in a computer fraud provision of a commercial crime coverage section of a policy may entitle the insured to coverage for ransomware attack, and denying summary judgment for both parties to determine if access to the insured's system was the result of a "trick"); RealPage Inc. v. Nat'l Union Fire Ins. Co., 21 F.4th 294, 299 (5th Cir. 2021) (no coverage for phishing scheme that resulted in loss of client funds that RealPage did not "hold" or own, despite policyholder having authority to direct transfer of funds from third-party processor's account); *see also* Metal Pro Roofing, LLC v. Cincinnati Ins. Co., 130 N.E.3d 653, 658–59 (Ind. Ct. App. 2019), *reh'g denied* (Nov. 7, 2019) (allowing policyholder to continue suit against insurer for fraudulent inducement alleging insured relied on the insurer's "quotes" describing its "Crime Expanded Coverage" as protecting against "computer hackers," even though the policy as issued arguably did not include such coverage).

144. *See, e.g.*, Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012) (affirming district court's grant of summary judgment for the insured and upholding ruling that commercial crime policy, which included a computer and funds transfer fraud endorsement, covered third-party costs resulting from data breach and hacking attack).

145. *See, e.g.*, State Bank of Bellingham v. BancInsure, Inc., 823 F.3d 456, 461 (8th Cir. 2016) (finding coverage under insured's financial institution bond for fraudulent transfer caused by computer virus, reasoning that "the computer systems fraud was the efficient and proximate cause of [the] loss," regardless of whether other non-covered causes contributed); Complaint, Ameriforge Grp., Inc. v. Fed. Ins. Co., No. 2016-00197 (Tex. Dist. Ct. Harris Cty. Jan. 4, 2016) (alleging that defendant breached its contract by denying coverage for inadvertent wire transfer prompted by fraudulent email); Ad Advert. Design, Inc. v. Sentinel Ins. Co., 344 F. Supp. 3d 1175 (D. Mont. 2018) (emails impersonating CEO that directed employee to wire funds to fraudulent account covered under theft of "money" and forgery provisions, but not under computer fraud provision that required "physical loss"); Ryeco, LLC v. Selective Ins. Co., 539 F. Supp. 3d 399, 407–08 (E.D. Pa. 2021) (no coverage under "Forgery or Alteration" section because "alteration" was of emails, not negotiable instruments as required under crime policy). *See also infra* note 157 and accompanying text.

146. G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 88–89 (Ind. 2021) (finding that "fraudulently cause a transfer" language in a computer fraud provision of a commercial crime coverage section of a policy

use of email in a fraudulent scheme is not enough to trigger such coverage if the email use was "merely incidental" to the fraud.[147]

While the courts have recognized that the concept of a crime policy seems on its face to encompass theft of confidential information, some crime policies specifically exclude theft of cyber or

---

may entitle the insured to coverage for ransomware attack, and denying summary judgment for both parties to determine if access to the insured's system was the result of a "trick"). *But see* SJ Computs., LLC v. Travelers Cas. & Sur. Co. of Am., No. 21-CV-2482 (PJS/JFD), 2022 WL 3348330, at *3–6 (D. Minn. Aug. 12, 2022) (crime policy's computer fraud coverage did not apply to loss caused by fraudulent invoices sent by email, but its social engineering coverage applied).

147. *See, e.g.*, Interactive Commc'ns, Int'l, Inc. v. Great Am. Ins. Co., 731 F. App'x 929, 935 (11th Cir. 2018) (denying coverage under crime policy because the loss was "temporally remote" and "intermediate steps, acts, and actors [made] clear" that the loss was not directly caused by computer fraud); Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 258 (5th Cir. 2016) (holding "Computer Fraud" provision of insured's crime protection insurance policy did not cover criminal transfer of funds involving an email, where the email was "merely incidental" to the crime); *see also* InComm Holdings, Inc. v. Great Am. Ins. Co., No. 1:15-cv-2671-WSD, 2017 U.S. Dist. LEXIS 38132 (N.D. Ga. Mar. 16, 2017), *aff'd*, No. 17-11712, 2018 U.S. App. LEXIS 12410 (May 10, 2018) (denying coverage under policy's "Computer Fraud" provision where the fraud was committed by phone, even though the transactions at issue were processed by computer); Miss. Silicon Holdings, LLC v. Axis Ins. Co., 843 F. App'x 581, 584–85 (5th Cir. 2021) (denying coverage under "Computer Transfer Fraud" provision where email scheme permitted fraudsters to monitor and alter emails but did not result in the manipulation of the insured's "system").

But see Principle Sols. Grp., LLC v. Ironshore Indem., Inc., 944 F.3d 886, 893 (11th Cir. 2019) (in construing ambiguity in favor of coverage, court found that despite employee interactions in response, the "loss unambiguously resulted directly from the fraudulent instruction") (quotation omitted); G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 98 (Ind. 2021) (transfer of bitcoin in response to ransomware involved "use of computer"); Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc., 23 F.4th 1195, 1201–03 (9th Cir. 2022) (finding email scheme in which imposter posed as employee's superior and directed her to make fraudulent payments resulted in a direct loss covered under the policy's "Computer Fraud Provision" and "Funds Transfer Fraud Clause"); City of Unalaska v. Nat'l Union Fire Ins. Co., No. 3:21-CV-00096-SLG, 2022 WL 826501, at *7–8 (D. Alaska Mar. 18, 2022) (use of computer in fraudulent email scheme was not incidental, but rather loss resulted "directly from" use of computer; court found proximate cause standard was sufficient).

intellectual property.[148] Even when this is not the case, these policies often limit coverage to theft of physical things or cash or securities.[149]

A case involving Bitcoin highlights the complexity of defining cyber assets in traditional first-party coverages. In *Kimmelman v. Wayne Insurance Group*,[150] Kimmelman submitted a claim under his homeowner's insurance for a stolen Bitcoin that he claimed was worth $16,000. The insurer investigated the claim and paid $200, which was the policy sublimit applicable to a loss of "money."[151] The insured filed suit and the insurer moved to dismiss, relying primarily on articles from CNN, CNET and the *New York Times* that apparently referred to Bitcoin as money, and an IRS document that "subscribed to Bitcoin and other electronic property" as "virtual currency."[152] Noting that there was no applicable legal authority except the IRS notice, the court found that Bitcoins were not "currency" because it is not recognized by the United States but that it

148. *See, e.g.*, Cargill, Inc. v. Nat'l Union Fire Ins. Co., No. A03-187, 2004 Minn. App. LEXIS 33, at *18 (Ct. App. Jan. 13, 2004) (crime policy specifically excluded "loss resulting directly or indirectly from the accessing of any confidential information, including, but not limited to, trade secret information, computer programs, confidential processing methods or other confidential information of any kind"); Ins. Servs. Office, Inc., Commercial Crime Coverage Form CR 00 20 05 06 § (F)(15) (2008), *available at* LEXIS, ISO Policy Forms (explicitly excludes computer programs and electronic data from the definition of "property"). *But see* Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012) (finding coverage under computer fraud rider to blanket crime policy for losses from hacker's theft of customer credit card and checking account data).

149. *See, e.g.*, People's Tel. Co. v. Hartford Fire Ins. Co., 36 F. Supp. 2d 1335 (S.D. Fla. 1997) (lists of cell phone serial and identification numbers were not "tangible property," so no crime policy coverage); Ryeco, LLC v. Selective Ins. Co., 539 F. Supp. 3d 399, 407–08 (E.D. Pa. 2021) (finding that "Forgery or Alteration" provision of crime policy did not include fraudulent Wire Transfer Authorization Forms because they are not negotiable instruments "similar to checks, drafts or promissory notes"); Ins. Servs. Office, Inc., Commercial Crime Coverage Form CR 00 20 05 06 § (A)3–8; § (F)(15) (2008) (coverage is for loss of money or securities, fraud, and theft of "other property," which is defined as "any tangible property other than 'money' and 'securities' that has intrinsic value" but excluding computer programs and electronic data).

150. Kimmelman v. Wayne Ins. Grp., No. 18 CV 1041, 2018 WL 7252940 (Ohio Ct. Com. Pl. Sept. 25, 2018).

151. *Id*. at *1.

152. *Id*.

was "property" because the IRS had taken the position that "for federal tax purposes, virtual currency is treated as property."[153]

Additionally, some policies contain an exclusion for actions of "authorized personnel"[154] or a requirement that an insured have no knowledge or consent to the crime.[155] These kinds of requirements can present difficult issues where coverage is sought under crime

---

153. *Id*. at *2. As such, the insurer's motion for judgment on the pleadings was denied. *See also AA v. Persons Unknown [2019] EWHC 2556 (Comm)* (bitcoin paid in response to ransomware attack held to be property under English law, and thus capable of being the subject of an injunction, because, while bitcoin is "virtual, not tangible and cannot be possessed," it has the recognized traits of property, namely "being definable, identifiable by third parties, capable of assumption . . . and having some degree of permanence"); G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82 (Ind. 2021) (finding bitcoin paid as ransom to hackers controlling insured's computer system was a loss under the policy).

154. *See, e.g.*, S. Cal. Counseling Ctr. v. Great Am. Ins. Co., 667 F. App'x 623 (9th Cir. 2016); Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co., No. C14-1368RSL, 2016 U.S. Dist. LEXIS 88985 (W.D. Wash. July 8, 2016), *aff'd*, 719 F. App'x 701 (9th Cir. 2018) (policy excluded loss involving person with authority); Universal Am. Corp. v. Nat'l Union Fire Ins. Co., 38 Misc. 859 (N.Y. Sup. Ct. 2013) (policy contained authorized personnel exclusion).

155. *See, e.g.*, Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627 (9th Cir. 2017) (rejecting coverage because the insured had knowledge of the wire transfer, even though no knowledge that the instructions were fraudulent); State Bank of Bellingham v. BancInsure, Inc., No. 13-cv-0900, 2016 U.S. Dist. LEXIS 94688 (D. Minn. July 19, 2016) (coverage found when computer hacker, not insured, made a fraudulent wire transfer), *aff'd*, 823 F.3d 456 (8th Cir. 2016); *see also* Pestmaster Servs., Inc. v. Travelers Cas. Sur. Co., 656 F. App'x 332, 333 (9th Cir. 2016) (no coverage because insured authorized transfer, and "fraudulently cause a transfer" language requires "an unauthorized transfer of funds"); Midlothian Enters., Inc. v. Owners Ins. Co., 439 F. Supp. 3d 737, 742–43 (E.D. Va. 2020) (denying coverage under exclusion for a "voluntary parting induced by any dishonest act" where employee wired money to another account due to an email from fraudster posing as firm's president); Miss. Silicon Holdings, LLC v. Axis Ins. Co., 843 F. App'x 581, 585–86 (5th Cir. 2021) (denying coverage under "Computer Transfer Fraud" provision where insured's employees approved the transfer of funds as a result of an email scam because coverage applied only to fraudulent transfers that caused a funds transfer "*without* [the insured entity's] knowledge or consent"); SJ Computs., LLC v. Travelers Cas. & Sur. Co. of Am., No. 21-CV-2482 (PJS/JFD), 2022 WL 3348330, at *3–6 (D. Minn. Aug. 12, 2022) (coverage under "Social Engineering Fraud" provision where CEO was duped into sending payments to hackers impersonating a vendor but no coverage under higher limits of "Computer Fraud" coverage because the policy excluded losses made by an "Employee [or] Authorized Person" or resulting from fraudulent instructions).

policies for "social engineering"[156] losses in which an authorized employee is duped into approving the transfer of confidential information or funds.[157]

---

156. Social Engineering Fraud "refers to the scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and funds." Interpol, www.interpol.int/Crimes/Financial-crime/Social-engineering-scams (social engineering fraud). *See also supra* note 155.

157. *Compare* Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., 719 F. App'x 701, 702 (9th Cir. 2018) (coverage barred because losses from a fraudulent email scam were not "direct[ly]" the result of crime since "Aqua Star's losses resulted from employees authorized to enter its computer system changing wiring information and sending four payments to a fraudster's account"); Sanderina, LLC v. Great Am. Ins. Co., No. 218CV00772JADDJA, 2019 WL 4307854, at *3–4 (D. Nev. Sept. 11, 2019) (denying coverage under crime policy for losses sustained when a third party posing as the company owner tricked an employee into transferring money to the imposter because scheme did not fit policy definitions); Star Title Partners of Palm Harbor, LLC v. Ill. Union Ins. Co., No. 8:20-CV-2155-JSM-AAS, 2021 WL 4509211, at *4–5 (M.D. Fla. Sept. 1, 2021) (denying coverage because fraudulent party did not purport to be insured's employee, customer, client, or vendor, and insured failed to authenticate the transfer pursuant to its own procedures, as required by the policy); *and* Midlothian Enters., Inc. v. Owners Ins. Co., No. 3:19-CV-51, 2020 WL 836832, at *4 (E.D. Va. Feb. 20, 2020) (no coverage for voluntary parting of funds by employee), *with* Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 480 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018) (finding coverage for the policyholder because the fraudulently induced transfer was a covered computer fraud under its crime policy: "The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high-level employees' knowledge and consent which was only obtained by trick."); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 462, 465 (6th Cir. 2018) (finding the insured suffered a direct loss because there was no intervening event where an impersonator posed as a vendor and tricked an employee into transferring funds to the fraudster's account and because the loss was "directly caused by computer fraud" in that the money was immediately lost upon transfer); Principle Sols. Grp., LLC v. Ironshore Indem., Inc., 944 F.3d 886, 893 (11th Cir. 2019) (in construing ambiguity in favor of coverage, court found that despite employee interactions in response, the "loss unambiguously resulted directly from the fraudulent instruction") (quotation omitted); Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc., 430 F. Supp. 3d 116, 130 (E.D. Va. 2019) (finding coverage where imposter impersonated insured's vendor through e-mail to initiate a fraudulent computer transfer because there was a "straightforward" or "proximate" relationship between use of any computer and the resulting loss); Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc., 23 F.4th 1195, 1201–03 (9th Cir. 2022) (email scheme in which imposter posed as

§ 16:3 Modern Cyber Policies

While some specialized coverages, such as errors and omissions (E&O) insurance in the medical or fiduciary context,[158] specifically include cyber and privacy risks inherent in the activity on which coverage is focused, as discussed above, traditional policy forms often impose significant limitations on coverage for these kinds of risks.[159] Indeed, gaps in traditional insurance for cyber and privacy risks may continue to widen as insurers increase the number of exclusions designed to limit coverage for these kinds of claims under traditional policies and seek to confine coverage for cyber and privacy to policies specifically designed for this purpose.[160]

In response to the coverage gaps created by evolving exclusions and policy definitions, the market for cyber insurance policies has responded with a host of new policies.[161] One survey indicated that more than 130 insurers now offer stand-alone cyber policies, many of which are manuscripted, and another found that the number of cyber insurance policies in force increased from 2.2 million in 2016 to more than 3.6 million in 2019.[162]

These cyber policy offerings are typically named peril policies that offer coverage on a claims-made basis. However, because of the

---

employee's superior and directed her to make fraudulent payments resulted in a direct loss covered under the policy's "Computer Fraud Provision" and "Funds Transfer Fraud Clause"); *and* City of Unalaska v. Nat'l Union Fire Ins. Co., No. 3:21-CV-00096-SLG, 2022 WL 826501, at *7–8 (D. Alaska Mar. 18, 2022) (finding coverage where imposter impersonated insured's vendor through email because the insured experienced a loss of money "resulting directly from" use of a computer). *See also infra* note 276 and accompanying text.

158. *See supra* section 16:2.3[B].

159. *See supra* section 16:2.

160. *See supra* notes 11, 25, 28, 46, 72, 87, and 149.

161. *See, e.g.*, *Types of Cyber Insurance*, CYBER INSURE ONE, https://cyberinsureone.com/types/; *Cyber Insurance*, AIG, www.aig.com/business/insurance/cyber-insurance; Chubb CyberSecurity Form 14-02-14874, § I.J. (2009); PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § I.C. (2010); *see also* RICHARD S. BETTERLEY, THE BETTERLEY REPORT: CYBER/PRIVACY INSURANCE MARKET SURVEY 2015 (June 2015) (surveying over thirty carriers that offer cyber insurance products), http://betterley.com/samples/cpims15_nt.pdf; *see also supra* note 11.

162. *See* Karin S. Aldama et al., *Seeing Around the Cyber Corner: What's Next for Cyber Liability Policies?*, ABA Ins. Coverage (May 31, 2018), www.americanbar.org/groups/litigation/committees/insurance-coverage/articles/2018/spring2018-cyber-liability.html; U.S. Gov't Accountability Office, GAO-21-477, *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market* (May 2021).

ever-evolving nature of the risks presented and the lack of standard policy terms, these offerings are in an ongoing state of flux as insurers continue to change and refine their policy forms. Various policy forms may be better suited to particular policyholders, businesses, and risk profiles.[163]

§ 16:3.1 Key Concepts in Cyber Coverage

As noted above, two important features of cyber policies are that they are often named peril policies and written on a claims-made basis.

[A] Named Peril

Although the distinction between all-risk and named-peril policies is based on conceptual frameworks that developed largely in the first-party context and many policies are hybrids that do not fall neatly in one category or the other, insurance policies are often categorized as either all-risk or named-peril policies.

All-risk policies typically cover all risks in a particular category unless they are expressly excluded. For example, the classic all-risk property policy covers "all risk of direct physical loss or damage" to covered property unless excluded.[164] These policies are said to offer broad and comprehensive coverage.[165]

Named-peril policies, on the other hand, cover only specified "perils" or risks. In the traditional property context, this may have been wind, storm, and fire, with some policies covering floods while

---

163. *Demystifying Cyber Insurance Coverage* (July 2022), DELOITTE, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-demystifying-cyber-insurance-coverage-report.pdf, at 8 (explaining that many cyber insurance policies lack standardization and offer vastly different levels of coverage). A white paper published by Wells Fargo noted that survey respondents' biggest challenge to purchasing cyber coverage was finding a policy that fit the company's needs (47% of respondents). Dena Cusick, *2015 Cyber Security and Data Privacy Survey: How Prepared Are You?*, at 3 (Wells Fargo, White Paper Sept. 2015). *See also infra* sections 16:3.2[A] and [B].

164. *See, e.g.*, City of Burlington v. Indem. Ins. Co. of N. Am., 332 F.3d 38, 47 (2d Cir. 2003) ("All-risk policies . . . cover all risks except those that are specifically excluded.").

165. *See, e.g.*, Villa Los Alamos Homeowners Ass'n v. State Farm Gen. Ins. Co., 130 Cal. Rptr. 3d 374, 382 (Ct. App. 2011) ("Coverage language in an all risk . . . policy is *quite broad*, generally insuring against all losses not expressly excluded."). *See generally* 7 COUCH ON INSURANCE § 101:7 (3d ed. Updated Online June 2022).

others do not. Unlike all-risk policies, named-peril policies do not typically provide coverage for risks other than the named perils.[166]

Cyber policies are generally named-peril policies, at least in the first-party property context, and different carriers have used dramatically different policy structures and definitions to describe what they cover and what they do not. Some of the more typical areas of coverage include:

First-party coverages

- costs of responding to a data breach, including privacy notification expenses, credit monitoring, and forensics
- loss of electronic data, software, hardware, and costs of reconstructing data
- loss of use and business interruption (including lost profits and continuing expenses)
- costs of data security and privacy events

---

166. *See, e.g.*, Burrell Commc'ns Grp. v. Safeco Ins., No. 94 C 3070, 1995 U.S. Dist. LEXIS 11699, at *3 (N.D. Ill. Aug. 10, 1995) (the insurance policy at issue was "an enumerated perils policy, meaning that only certain named perils are covered"). *See generally* 4 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 29.01(3)(b)(1) (2020) ("'named peril' policies . . . cover only the damages that result from specific categories of risks, and 'all risks' policies . . . cover the damages from all risks except those specifically excluded by the policy"). A number of cases have decided that crime policies may contain specific policy definitions that limit coverage by the type of cyber or computer fraud loss and the methods by which the crime is perpetrated. *See, e.g.*, Sanderina, LLC v. Great Am. Ins. Co., No. 218CV00772JADDJA, 2019 WL 4307854, at *3–4 (D. Nev. Sept. 11, 2019) (denying coverage for losses sustained when a third party posing as the company owner tricked an employee into transferring money to the imposter because the scheme did not fit the definitions for the three relevant policy provisions: (1) "emails containing directions are not similar to checks or drafts" under the forgery provision; (2) no "direct access" to the company's computer system occurred as required by the computer fraud provision; and (3) the instructions were not sent to a "financial institution" or without "knowledge or consent" as required by the funds-transfer fraud provision); Ryeco, LLC v. Selective Ins. Co., 539 F. Supp. 3d 399, 407–08 (E.D. Pa. 2021) (finding that "Forgery or Alteration" provision of crime policy did not include fraudulent Wire Transfer Authorization Forms because they are not negotiable instruments "similar to checks, drafts or promissory notes"); *see also* P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016), *appeal dismissed*, No. 16-16141 (9th Cir. Jan. 27, 2017), ECF No. 15 (discussed in *infra* section 16:3.2[O]).

- loss from cyber crime
- rewards for responding to cyber threats and extortion demands
- public relations for cyber risks

Third-party coverages

- suits against insured for data breach or defamation
- liability for loss of another's electronic data, software, or hardware, resulting in loss of use
- loss of funds of another due to improper transfer
- data security and privacy injury
- statutory liability under state and federal privacy laws
- advertising injury
- intellectual property infringement

Governmental action may fall in both first- and third-party coverages depending on particular policy wording.

[B] Claims Made

Most cyber liability policies are claims-made policies, which in very general terms means that the policy is triggered by a claim made and, in some cases, noticed during the policy period.[167] Most claims-made policies contain provisions, commonly known as "tail" provisions, which provide an extended reporting period during which an insured can give notice of a claim made after the end of the policy period that alleges a wrongful act before the policy period ended.[168] But even here, there is often a specific time span in which notice must be given to the insurer.[169]

Claims-made policies are distinguished from occurrence policies, which are typically triggered by an event or damage during the policy period, regardless of when the occurrence is known to the insured

---

167. *See generally* 2 RONALD N. WEIKERS, DATA SEC. AND PRIVACY LAW § 14:36 (2015). Some first-party cyber coverages are triggered by discovery during the policy period of the cyber event.
168. *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 16.07 (2020).
169. *See, e.g.*, Prodigy Commc'ns Corp. v. Agric. Excess & Surplus Ins. Co., 288 S.W.3d 374, 375 (Tex. 2009) (claims-made policy's tail provision required insured to give notice of a claim "as soon as practicable . . . , but in no event later than ninety (90) days after the expiration of the Policy Period" which the court found binding).

or notified to the insurer.[170] In some cases, such as mass torts, environmental contamination or asbestos, occurrence policies in effect at the time of the contamination or exposure to an allegedly dangerous product or substance can cover claims asserted decades later when the contamination is discovered or the policyholder is sued by a claimant who alleges recent diagnosis of illness.[171] Use of a claims-made form allows the insurer to attempt to limit exposure to the policy period (and any tail period) without having to wait many years to see if a data breach is later discovered to have occurred during the period when the policy was in effect.

In addition to having dates by which notice must be given, many claims-made policies have "retro" dates that preclude claims for breaches prior to a designated date, regardless of when the claim is asserted and noticed to the insurer.[172] Often, these retro dates are designed to limit coverage to the first time a particular carrier began issuing claims-made coverage to a particular insured.

Some policies include provisions under which subsequently asserted claims may be deemed to have been made in an earlier policy period because they "relate back" to an earlier, related incident.[173]

---

170. *See generally* 3 ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 11.5 (6th ed. Updated Online Mar. 2022).

171. *See, e.g.*, Scott's Liquid Gold, Inc. v. Lexington Ins. Co., 293 F.3d 1180, 1182–83 (10th Cir. 2002) (upholding a decision finding insurer has a duty to indemnify insured for occurrence of pollution into soil and groundwater in the 1970s, even though the action was brought in 1994); Keene Corp. v. Ins. Co. of N. Am., 667 F.2d 1034, 1040 (D.C. Cir. 1981) (finding insurer liable for injuries, as defined by the policy, that caused asbestos-related harm many years after inhalation in an occurrence policy). *See generally* 4 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 27.01 (2020).

172. *See, e.g.*, City of Shawnee v. Argonaut Ins. Co., 546 F. Supp. 2d 1163, 1181 (D. Kan. 2008) (policy contains "a Retroactive Date–Claims Made Coverage endorsement"); Coregis Ins. Co. v. Blancato, 75 F. Supp. 2d 319, 320–21 (S.D.N.Y. 1999) ("'Retroactive Date' is defined in the policy as: the date . . . on or after which any act, error, omission or PERSONAL INJURY must have occurred in order for CLAIMS arising therefrom to be covered under this policy. CLAIMS arising from any act, error, omission or PERSONAL INJURY occurring prior to this date are not covered by this policy."). *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN INSURANCE LAW PRACTICE GUIDE § 16.07 (2020).

173. *See, e.g.*, WFS Fin. Inc. v. Progressive Cas. Ins. Co., No. EDCV 04-976-VAP(SGLx), 2005 U.S. Dist. LEXIS 46751, at *6 (C.D. Cal. Mar. 29, 2005) (D&O policy stated: "Claims based upon or arising out of the same Wrongful Act or Interrelated Wrongful Acts committed by one or more of the Insured Persons shall be considered a single Claim, and only one Retention and Limit of Liability shall be applicable. However, each such single claim shall be deemed to be first made on the date the

These provisions are commonly referred to as "related acts" or "interrelated acts" clauses and are often found in claims-made policies, including cyber policies.[174] Such clauses are particularly relevant in the cyber context, because the forensic investigations that follow a breach may unearth indicia that a different, arguably related breach also occurred. Common elements that may be asserted to trigger a related acts provision may include the attack vector, the identity of the hacker, the vulnerability in the software or hardware that led to the attack, or the type of information compromised.[175]

Under some policies, it may also be possible to provide a notice of circumstance that may lead to a claim, which will bring claims asserted after the policy expires into the policy period when the notice was given.[176] Such notices are often at the discretion of the insured,[177] but sometimes raise issues as to the level of particularity required for such notices to be effective.[178]

---

earliest of such Claims was first made, regardless of whether such date is before or during the Policy Period."), *aff'd*, 232 F. App'x 624 (9th Cir. 2007).

174. *See, e.g.*, Travelers CyberRisk Form CYB-3001, § II.WW (ed. 07-10), www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-3001.pdf ("Related Wrongful Act means all Wrongful Acts that have as a common nexus, or are causally connected by reason of, any act or event, or a series of acts or events.").

175. While there is a dearth of case law on this point specific to cyber policies, cases interpreting similar provisions in D&O policies may prove instructive. *See, e.g.*, BAILEY, DAN A., LIABILITY OF CORPORATE OFFICERS AND DIRECTORS § 24.05 (2020). *Compare, e.g.*, WFS Fin. Inc. v. Progressive Cas. Ins. Co., 232 F. App'x 624, 625 (9th Cir. 2007) (two different suits were "Interrelated Wrongful Acts" despite fact that "the suits were filed by two different sets of plaintiffs in two different fora under two different legal theories" because "the common basis for those suits was the [insured's] business practice of permitting independent dealers to mark up [the insured's] loans"), *with* Nat'l Union Fire Ins. Co. v. Ambassador Grp., Inc., 691 F. Supp. 618, 623–24 (E.D.N.Y. 1988) (claims were *not* "interrelated acts" despite fact that they "all involve allegations of wrongdoing of one sort or another and relate, in some way, to the demise of [the insured] and its subsidiaries" because the claims were "legally distinct claims that allege different wrongs to different people").

176. *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 20.01 (2020).

177. *See, e.g.*, AIG, Specialty Risk Protector, CyberEdge Security and Privacy Liability Insurance, General Terms and Conditions § 6(c) (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf (giving insured option to provide notice "of any circumstances which may reasonably be expected to give rise to a Claim").

178. *See, e.g.*, JPMorgan Chase & Co. v. Travelers Indem. Co., 73 A.D.3d 9 (N.Y. App. Div. 1st Dep't 2010) (insurer argued that notice of circumstances was deficient because it was vague and based on conjecture).

§ 16:3.2 Issues of Concern in Evaluating Cyber Risk Policies

Though they vary in structure and form, the new cyber risk policies raise a variety of issues, some of which are akin to issues posed by more traditional insurance policies and some of which are unique to these new forms.

[A] What Is Covered?

As noted above, cyber policies are, at least in some respects, named-peril policies.[179] In other words, they generally cover specifically identified risks. In order to determine the utility of the coverage being provided, a policyholder should assess carefully its own risks and then compare them to the protections provided by a particular form.[180] For example, a company in the business of providing cloud computing services to third parties gains limited protection from a policy that specifically excludes, or does not cover in the first place, liabilities to third parties due to business interruption. On the other hand, a company that is highly reliant on cloud providers is left with substantial uninsured risk if its cyber policy does not cover loss of information or disruption of its cloud provider.[181] In another illustration of the issue, the array of problems and issues faced by policyholders that sell computer services are different from those of companies that sell no services but handle a great deal of statutorily protected medical or personal financial information. The availability of coverage may also depend on the kind of computer infrastructure involved. Given all the permutations, the first step in analyzing any cyber policy is to compare the risks of the policyholder at issue to the specific coverages under consideration.

[B] Confidential Information, Privacy Breach, and Other Key Definitions

In most cyber policies, there are key definitions such as confidential information, personal identifiable information, computer or

---

179. *See supra* section 16:3.1[A].

180. In an example of insurance products evolving to meet specific needs, there are now numerous types of cyber security policies for specific cyber events. *See Types of Cyber Insurance*, CYBER INSURE ONE, https://cyberinsureone.com/types/; *Cyber Insurance*, AIG, www.aig.com/business/insurance/cyber-insurance.

181. *See* CRC GROUP, STATE OF THE MARKET: IS MY CLOUD STACK INSURED BY CYBER COVERAGE? (2016), www.crcins.com/docs/professional/Cloud_Stack.pdf (discussing the issue of insuring against contingent business interruption losses if a major cloud provider, like Amazon Web Services, were to suffer an outage or privacy breach).

computer system,[182] and privacy or security breach that are crucial to analyzing and understanding the coverage offered. In some cases, policy language ties these definitions to statutory schemes in the United States and abroad that themselves continue to be in flux.[183]

However they are drafted, these key definitions and their applicability can be very technical and should be reviewed by both insurance and technology experts to ensure that the risks inherent in a particular technology platform are adequately covered. This is particularly true as more and more businesses rely on third-party providers or affiliated entities within a corporate family for technology services. For example, some policies may cover leased computers or information in the hands of vendors while other policies may not. Coverage for data in the hands of a third party may require memorialization of the relationship in a written contract. Careful vetting of these key definitions is essential to understanding and negotiating coverage.

---

182. *See* U.S. Gov't Accountability Office, GAO-21-477, *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market* (May 2021) (noting that the lack of common terminology makes it difficult to understand coverage and suggesting standardization would increase clarity and transparency). *See, e.g.*, Response in Opposition to Plaintiff's Motion for Partial Summary Judgment at 6, Hub Parking Tech. USA, Inc. v. Ill. Nat'l Ins. Co., No. 2:19-cv-00727 (W.D. Pa. Dec. 3, 2019), ECF No. 32 (arguing that printing receipts containing customers' credit card numbers did not qualify as a "security failure" under the policy definition because there was no allegation of unauthorized access or unauthorized use of the computer system), *dismissed*, No. 2:19-cv-00727 (W.D. Pa. June 25, 2020), ECF No. 54 (parties settled and agreed to a stipulation of dismissal).

183. As of December 2019, all fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands had security breach notification laws, and in 2019, at least thirty-one states considered revisions to their existing security breach laws. *2019 Security Breach Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Dec. 31, 2019), www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx. *See also* Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1 (GDPR became effective on May 25, 2018, and deals with processing the personally identifiable information of individuals residing in the European Union, regardless of where a company is located). *See infra* section 16:3.3.

[C] Overlap with Existing Coverage

One of the difficult issues with the new cyber policies is determining what coverage they provide in comparison to the insurance provided by traditional policies. Most risk managers do not want to pay for the same coverage twice, much less to have two carriers arguing with each other as to which is responsible, or about how to allocate responsibility between them for a particular loss.

Many brokers prepare analyses for their clients of the interplay between traditional coverages and cyber policies, and these comparisons should be considered carefully to avoid multiple and overlapping coverages for the same risks. Examples of potential overlaps may include: physical destruction to computer equipment covered by property and cyber policies; disclosure of confidential personal information potentially covered by CGL, E&O, and cyber policies; and theft of computer resources or information under crime and cyber policies. The extent of any overlap among these or other coverages may only be identified by careful analysis. Indeed, insurers have sometimes argued that the availability of cyber policies in the marketplace should support a restrictive reading of traditional insurance products.[184]

[D] Limits and Deductibles

Because cyber policies are typically structured as named peril policies, they often have specific limits or sublimits as well as deductibles for each type of coverage. Some cyber policies are crafted for "low frequency but high severity" cyber events affecting large amounts of electronic data.[185] However, many companies face repeated smaller-scale data breaches and need to consider deductible structures that provide coverage for these costs.[186] Primary and

---

184. *Compare* G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 87–88 (Ind. 2021) (insurer argued unsuccessfully that fact that insured was offered but declined to purchase optional "computer virus and computer hacking coverage" showed that computer viruses and computer hacking were meant to be excluded from crime policy's coverage), *with* Ryeco, LLC v. Selective Ins. Co., 539 F. Supp. 3d 399, 407–08 (E.D. Pa. 2021) (finding sections of crime policy did not overlap, and denying coverage under "Forgery and Alteration" provision where "Funds Transfer Fraud" provision would have covered loss resulting from fraudulent emails directing bank to pay hackers' account).

185. *See* ADVISEN, MITIGATING THE INEVITABLE: HOW ORGANIZATIONS MANAGE DATA BREACH EXPOSURES (Mar. 2016), www.advisenltd.com/wp-content/uploads/2016/03/how-organizations-manage-data-breach-exposures-2016-03-03.pdf.

186. *See id*.

excess limits associated with a particular coverage also must be reviewed to ensure adequate coverage for risks of concern.

One issue that often arises in traditional policies, and may also arise in the cyber context, is whether an insured's losses are subject to multiple sublimits or deductibles. For example, an insured's policy may contain multiple "sublimits," or "per claim" or "per occurrence" deductibles[187] that apply to losses in various categories.[188] Depending on the policy form, there may be arguments as to whether the insured is entitled to collect under multiple sublimits or whether the entirety of the insured's losses are capped by one of the sublimits in question.[189] Similar issues may arise when the policy contains multiple potentially applicable deductibles.[190] When negotiating a cyber policy, it is important that the policy make clear how multiple sublimits and deductibles will apply in such situations. Where a policy has sublimits, excess policies should be reviewed to ensure that they attach in excess of relevant sublimits and aggregate limits.

Another issue concerns a "related acts" or "interrelated acts" provision. As noted above,[191] these provisions sometimes aggregate losses from a single breach or related series of breaches into one claim or occurrence and thus may impact on the applicability of limits, sublimits, and retentions by aggregating losses from multiple incidents into a single claim or occurrence.[192]

---

187. *See, e.g.*, W. Heritage Ins. Co. v. Asphalt Wizards, 795 F.3d 832 (8th Cir. 2015) (deductible amount not met for TCPA violations due to $1000 per claim deductible); First Mercury Ins. Co. v. Nationwide Sec. Servs., 54 N.E.3d 323 (Ill. App. Ct.), *appeal denied*, 60 N.E.3d 872 (Ill. 2016) (applying a "per claim" deductible of $500 relating to TCPA damages).

188. *See, e.g.*, CNA Commercial Property Policy Form G-145707-C (2012).

189. *See, e.g.*, Hewlett-Packard Co. v. Factory Mut. Ins. Co., No. 04 Civ. 2791 (TPG) (DCF), 2007 WL 983990 (S.D.N.Y. 2007) (holding that insured was entitled to collect for property damage up to $50 million under its "electronic data processing" sublimit, as well as its additional losses for business interruption, which were not capped by the electronic data processing sublimit); Penford Corp. v. Nat'l Union Fire Ins. Co., 662 F.3d 497 (8th Cir. 2011) (the parties' mutual understanding that the sublimits in the policy capped coverage for both property damage and business interruption losses).

190. *See, e.g.*, Gen. Star Indem. v. W. Fla. Vill. Inn, 874 So. 2d 26 (Fla. Dist. Ct. App. 2004) (involving the issue of which deductible applied on a policy containing two different deductibles for different types of causes of loss).

191. *See supra* section 16:3.1[B].

192. *See supra* note 173 and accompanying text.

[E] Notice Requirements

As noted above, cyber policies are often claims-made policies.[193] But unlike many claims-made policies, particularly in the liability context, cyber policies sometimes require notice to insurers of known occurrences and lawsuits "as soon as practicable."[194] These clauses are most common where insurers are obligated to defend a claim, the insurers' view being that they want to know of the claim as early as possible in order to defend.

Putting aside issues of how soon is practicable,[195] a commonly encountered question is when the obligation to give notice is triggered. Practitioners often advise large corporate insureds to limit the obligation to give notice to when a specified individual or group of individuals—commonly the risk manager, CFO, CIO, or general counsel—has knowledge of the claim. This is especially important in large organizations where an individual who receives knowledge of an event, claim, or potential claim may not be in a position to give notice or even to understand that notice is required. Where policies contain these kinds of provisions, courts have repeatedly held them to be enforceable.[196]

---

193. *See supra* section 16:3.1[B].

194. *See, e.g.*, TRAVELERS, CyberRisk Form CYB-3001, § IV.E.1 (ed. 07-10), www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-3001.pdf (requiring notice "as soon as practicable"); AIG, Specialty Risk Protector § 6(a) 101013 (Dec. 2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf (as soon as practicable after knowledge or discovery).

195. *See* 8f-198 APPLEMAN ON INSURANCE § 4734 (2020) (what is immediate or practicable depends upon the facts of a particular case and does not require instantaneous notice); *see also* ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 1:1 (6th ed. Updated Online Mar. 2022) (the soon-as-practicable standard generally involves a consideration of what is reasonable given the circumstances). Many jurisdictions require the insurer to show prejudice to support a late notice defense. *See, e.g.*, Ins. Co. of Pa. v. Associated Int'l Ins. Co., 922 F.2d 516, 524 (9th Cir. 1990) ("Under California law, the insurer has the burden of proving actual and substantial prejudice."); Nat'l Sur. Corp. v. Immunex Corp., 297 P.3d 688, 696 (Wash. 2013) (same). However, policies requiring notice within the policy period or an extended reporting period are often enforced. *See, e.g.*, James & Hackworth v. Cont'l Cas. Co., 522 F. Supp. 785 (N.D. Ala. 1980) (enforcing provision that required insured to provide notice during the policy period or within sixty days after its expiration).

196. *See, e.g.*, Hudson Ins. Co. v. Oppenheim, 81 A.D.3d 427, 428 (N.Y. App. Div. 2011) (upholding a provision stating: "The subject policy required the insured to provide notice of a loss 'At the earliest practicable moment after discovery of loss by the Corporate Risk Manager,' and provided that 'Discovery occurs when the Corporate Risk Manager first becomes

The issue of whose knowledge triggers the obligation to give notice takes on particular significance in the cyber context. There may be a considerable lapse between the time of a covered event and the time when knowledge of that event surfaces. In some cases, knowledge of the event may be confined to front-line information technology personnel who are focused on containing the problem and have no familiarity with insurance or its requirements. As a result, policyholders may attempt to negotiate provisions in cyber policies that predicate notice requirements on knowledge by the risk manager, CFO, CIO, or similarly appropriate individuals. When the insurance policy contains such knowledge-based language, it may also be important to develop internal procedures to ensure that insurable claims or events are brought to the attention of such individuals.

[F] Coverage for Regulatory Investigations or Actions

A major issue in evaluating cyber insurance relates to the extent to which there is coverage for regulatory investigations or actions. As an example, the Federal Trade Commission (FTC) regularly files complaints or launches investigations, both formal and informal,[197] into company practices that may violate section 5 of the Federal Trade Commission Act ("FTC Act") by unfairly handling consumer information.[198] Other regulatory bodies have entered the

---

aware of facts.'"); QBE Ins. Corp. v. D. Gangi Contracting Corp., 888 N.Y.S.2d 474, 475 (App. Div. 2009) (enforcing an insurance policy stating: "Knowledge . . . by Your agent, servant or employee shall not in itself constitute knowledge of you unless the Corporate Risk Manager of Your corporation shall have received notice of such Occurrence.").

197. FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY (Sept. 13, 2021), www.ftc.gov/reports/ftc-report-congress-privacy-security (summarizing high-profile enforcement action taken by the agency). *See also* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2020 PRIVACY AND DATA SECURITY UPDATE (May 2021), www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf (describing FTC cybersecurity enforcement efforts over the past twenty years, including more than 130 spam and spyware cases and approximately eighty general privacy lawsuits).

198. The FTC's power was affirmed in FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015), where the federal court rejected a challenge to the FTC's authority to use its section 5 authority to sue merchants for data breaches. After Wyndham suffered several data breaches between 2008 and 2010, the FTC filed an action alleging that Wyndham engaged in unfair practices and that its privacy policy was deceptive. *Id*. at 240; *see also* Opinion at 1, *In re* LabMD, Inc., No. 9357 (FTC July 29, 2016)

fray as well.[199] For instance, new rules proposed by the Securities & Exchange Commission (SEC) would require periodic reporting regarding cybersecurity policies and procedures to identify risks, the role of the board of directors and management in overseeing and implementing cybersecurity controls, and disclosure of any director's

---

(concluding LabMD's security practices were unreasonable and lacked "even basic precautions" that could protect against a data breach; noting deficiencies with the company's failure to (1) use an intrusion-detection or file-monitoring system; (2) monitor traffic coming across its firewalls; (3) provide data security training to its employees; and (4) periodically delete consumer data that it had collected), *vacated sub nom.* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018) (finding unenforceable the FTC's cease and desist order for LabMD to implement security measures, noting that the FTC "mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished"); *In re* Flo Health, Inc., FTC File No. 1923133 (2021), www.ftc.gov/enforcement/cases-proceedings/1923133/flo-health-inc. (enforcement action against health app company alleging that health data of users of the company's Flo Period & Ovulation Tracker app was disclosed to third parties); *In re* Café Press, FTC File. No. 1923209 (2022), www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter (enforcement action alleging the company (1) failed to provide reasonable security for sensitive personal information of customers; (2) knowingly failed to provide timely notification to users of a breach involving millions of users' data; and (3) made deceptive statements about how customers' personal information would be used); *In re* Zoom Video Commc'ns, Inc., FTC File No. 1923167 (2020), www.ftc.gov/legal-library/browse/cases-proceedings/192-3167-zoom-video-communications-inc-matter (enforcement action against video conferencing provider, which alleged that Zoom misled consumers about the level of security provided to them and compromised security of Mac users, was settled after Zoom agreed to implement a comprehensive security program, review software for security flaws, and obtain biennial third-party assessments of its security program). In the agency's first children's privacy and security case, VTech Electronics settled a claim by the FTC alleging that the electronic toymaker collected personal information about children without providing notice and obtaining parental consent, and thereafter failed to adequately protect the information. United States v. VTech Elecs., Ltd., No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018).

199. For example, Excellus Health Plan Inc. reached a resolution with the U.S. Department of Health and Human Services in the wake of an investigation into a data breach Excellus reported in 2015 that exposed the data of over 9.3 million people and raised HIPAA violation concerns. Per the resolution, Excellus will be required to pay $5.1 million and undergo an in-depth risk analysis. Adam Lidgett, *Excellus to Pay $5.1M in HHS Deal over Data Hack*, LAW360 (Jan. 15, 2021), www.law360.com/articles/1345691/excellus-to-pay-5-1m-in-hhs-deal-over-data-hack.

cybersecurity expertise.[200] Cybersecurity cases have become a principal enforcement focus for the SEC, specifically relating to internal controls to protect market integrity and disclosure of material cyber events.[201] Likewise, the Financial Industry Regulatory Authority (FINRA) has stated that cybersecurity is an enforcement priority.[202]

State attorneys general also exercise investigative and prosecutorial powers in the cyber area, as do regulatory and law enforcement authorities around the globe.[203] For example, in July 2020, New York's Department of Financial Regulation filed charges against First American Title Insurance Company for allegedly violating the state's Cybersecurity Requirements for Financial Services Companies by failing to perform risk assessments and to properly test, identify, and remedy a website vulnerability that allowed unauthorized access to tens of millions of records containing consumers' sensitive data.[204] The Statement of Charges seeks remedy of the violations and "civil monetary penalties."[205]

In many instances, coverage for these kinds of situations will turn on the definition of "claim" in the relevant policy.[206] If, for example, a claim is defined as an action for civil damages, regulatory actions may not fall within that category.[207] Many cyber policies address this issue by including a broader definition of "claim" that encompasses criminal proceedings, claims for injunctive relief,

---

200. SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, U.S. SEC. & EXCH. COMM'N (Mar. 9, 2022), www.sec.gov/news/press-release/2022-39. *See also* Luis A. Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, Address at Cyber Risks and the Boardroom Conference: Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014), www.sec.gov/news/speech/2014-spch061014laa.

201. *Id*. *See also infra* section 16:3.3.

202. *See Report on Selected Cybersecurity Practices—2018*, FINRA (Dec. 2018), www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

203. *See, e.g.*, Josh Horowitz, *China passes new personal data privacy law, to take effect Nov. 1*, REUTERS (Aug. 20, 2021), www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/.

204. Statement of Charges, *In re* First Am. Title Ins. Co., No. 2020-0030-C (July 21, 2020), www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf.

205. *Id*.

206. *See also infra* note 282 (discussing exclusion for failure to consistently implement cyber risk controls).

207. *See, e.g.*, Passaic Valley Sewerage Comm'rs v. St. Paul Fire & Marine Ins. Co., 21 A.3d 1151, 1159 (N.J. 2011) (rejecting an insured's coverage for a claim for injunctive regulatory relief because, under the policy, a claim was defined as one for civil damages).

and certain administrative or regulatory proceedings as well.[208] In light of the increased regulatory activity around the world, including in the European Union and China, the definition of "claim" should be reviewed to determine the scope of coverage for actions or investigations by regulatory agencies globally.

As illustrated by various cases involving D&O liability policies, the definition of claim can be very important in establishing the degree of formality required for coverage to be available for a particular regulatory initiative. Some policies, for example, require the filing of a notice of charges, an investigative order, or similar document.[209]

---

208. *See, e.g.*, AIG CyberEdge Security and Privacy Liability Insurance, Form 101024 (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf ("Claim" means: (1) a written demand for money, services, non-monetary relief or injunctive relief; (2) a written request for mediation or arbitration, or to toll or waive an applicable statute of limitations; (3) a suit; or (4) a regulatory action [meaning "a request for information, civil investigative demand or civil proceeding brought by or on behalf of a governmental agency, including requests for information related thereto"]). Similarly, in the D&O context, see, e.g., Chubb Forefront for Insurance Companies Policy, Form 17-02-1716, § 36 (1999) ("Claim means: (a) a written demand for monetary damages; (b) a civil proceeding commenced by the service of a complaint or similar pleading; (c) a criminal proceeding commenced by the return of an indictment; or (d) a formal administrative or regulatory proceeding."); Liberty Mutual Group: Liberty Insurance Underwriters, Inc. General D&O Form US/D&O2000-POL (Ed. 1/00) (2004) ("The definition of claim includes a written demand for monetary or nonmonetary relief, a civil or criminal proceeding or arbitration, a formal administrative or regulatory proceeding, or a formal criminal, administrative investigation commenced.").

209. *Compare* AIG Executive Edge Public Company Directors & Officers Liability, Form 115485 (June 2013), § 14 (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/management-liability/portfolioselect-for-public-companies-specimen-policy-brochure.pdf (defines "claim" to include "proceedings" that are "commenced by (i) service of a complaint or similar pleading; (ii) return of an indictment, information or similar document (in the case of a criminal proceeding); or (iii) receipt or filing of a notice of charges."), *with* AIG Executive Liability, Directors, Officers and Private Company Liability Insurance, Form 95727 (Sept. 2007), § 2(b)(iii) (2007), https://eperils.com/app/95727.pdf (also includes within the definition of "claim" "investigations" of individual insureds once identified in writing by an investigatory authority, or served a subpoena or Wells notice by the Securities and Exchange Commission). *See also* Hertz Glob. Holdings, Inc. v. Nat'l Union Fire Ins. Co., No. 19-CV-06957 (AJN), 2021 WL 1198802, at *6–8 (S.D.N.Y. Mar. 30, 2021) (denying coverage for costs associated with an SEC investigation because (1) the investigation was not an administrative or regulatory proceeding,

Under such policies, a proceeding initiated by formal administrative action may be a precondition to coverage. This can be problematic because many administrative initiatives are informal and policyholders often prefer that they remain at an informal stage.

The issue is illustrated by cases like *Office Depot, Inc. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*[210] and *MBIA, Inc. v. Federal Insurance Co.*[211] In the *Office Depot* case, the policyholder sought coverage for an SEC investigation into assertions it had selectively disclosed certain non-public information in violation of federal securities laws.[212] While the SEC's investigation commenced in 2007, no subpoena was issued until 2008.[213] The policy contained coverage for a "securities claim," but the definition of "securities claim" specifically carved out "an administrative or regulatory proceeding against, or investigation of the [company]" unless "during the time such proceeding is also commenced and continuously maintained against an Insured Person."[214] Recognizing that the policy

---

and therefore did not meet the definition of "securities claims," and (2) although the policy covered investigations against covered individuals, the insured failed to sufficiently allege that the investigation was against individuals).

210. Office Depot, Inc. v. Nat'l Union Fire Ins. Co., 453 F. App'x 871 (11th Cir. 2011).

211. MBIA, Inc. v. Fed. Ins. Co., 652 F.3d 152 (2d Cir. 2011).

212. Office Depot, Inc. v. Nat'l Union Fire Ins. Co., 453 F. App'x 871, 871 (11th Cir. 2011).

213. *Id*. at 874.

214. As the court explained:

> Two policy provision[s] are relevant to the disposition of this issue. First, the insuring agreement language provides:
>
> > COVERAGE B: ORGANIZATION INSURANCE
> >
> > (i) *Organization Liability.* This policy shall pay the Loss of any Organization arising from a Securities Claim made against such Organization for any Wrongful Act of such Organization. . . .
>
> The policy defines a Securities Claim as:
>
> > a Claim, *other than an administrative or regulatory proceeding against, or investigation of an Organization*, made against any Insured:
> >
> > (1) alleging a violation of any federal, state, local or foreign regulation, rule or statute regulating securities . . . ; or
> > (2) brought derivatively on the behalf of an Organization by a security holder of such Organization.
>
> Notwithstanding the foregoing, the term "Securities Claim" *shall include an administrative or regulatory proceeding* against an Organization, but only if and only during the time such

provided coverage for regulatory or administrative "proceedings," the Eleventh Circuit held there was no coverage for administrative or regulatory "investigations"[215] until, here, the issuance of a subpoena.[216]

A different approach is illustrated by the *MBIA* case, in which the policyholder sought coverage for an SEC investigation.[217] While the SEC obtained a formal investigatory order, it did not issue subpoenas to MBIA because MBIA had asked the SEC to "accept voluntary compliance with their demands for records in lieu of subpoenas to avoid adverse publicity for MBIA."[218] The policy covered "any formal or informal administrative or regulatory proceeding or inquiry commenced by the filing of a notice of charges, formal or informal investigative order or similar document."[219] The insurers argued that because the SEC's investigation had proceeded through oral requests, as opposed to subpoenas or other formal processes, there was no coverage.[220] The Second Circuit held that the SEC's oral requests were issued pursuant to a formal investigative order and thus constituted securities claims under the policy.[221] The Second Circuit went on to state that "insurers cannot require that as an investigation proceeds, a company must suffer extra public relations damage to avail itself of coverage a reasonable person would think was triggered by the initial investigation."[222]

Modern policies, including cyber policies, have dealt with these issues in a variety of ways, including provisions providing explicit coverage for informal inquiries or the cost of preparing an individual to testify;[223] however, some of these provisions do not cover the

---

proceeding is also commenced and continuously maintained against an Insured Person.

Id. at 875 (footnotes omitted).

215. *Id*. at 877.

216. *Id*. at 878. *See also* Hertz Glob. Holdings, Inc. v. Nat'l Union Fire Ins. Co., No. 19-CV-06957 (AJN), 2021 WL 1198802, at *6–8 (S.D.N.Y. Mar. 30, 2021) (denying coverage for costs associated with an SEC investigation because (1) the investigation was not an administrative or regulatory proceeding, and therefore did not meet the definition of "securities claims," and (2) although the policy covered investigations against covered individuals, the insured failed to sufficiently allege that the investigation was against individuals).

217. MBIA, Inc. v. Fed. Ins. Co., 652 F.3d 152, 160 (2d Cir. 2011).

218. *Id*. at 156.

219. *Id*. at 159.

220. *Id*. at 161.

221. *Id*. at 162.

222. *Id*. at 161.

223. *See, e.g.*, AIG CyberEdge Security and Privacy Liability Insurance, Form 101024 (2013), www.aig.com/content/dam/aig/america-canada/us/

substantial costs that an insured company, as opposed to an insured individual, may be forced to incur, particularly where there is extensive electronic discovery or document production.[224] Insureds generally seek to procure insurance policies with a low threshold for what triggers coverage in relation to a regulatory investigation and broad definition of the agencies whose investigations will trigger the policy.

Another issue that sometimes arises when policyholders seek coverage for a regulatory investigation or action is whether there has been a "Wrongful Act" under the definition in the relevant policy. For example, in *Employers' Fire Insurance Co. v. ProMedica Health Systems, Inc.*,[225] the court considered whether there was coverage for an FTC antitrust investigation[226] that culminated in the FTC initiating an administrative proceeding against the policyholder.[227] The policy in *ProMedica* defined "Wrongful Act" to include "'any actual or alleged' antitrust violation."[228] The *ProMedica* court concluded that the FTC investigation was not "for a Wrongful Act" because the FTC did not "affirmatively accuse [the policyholder] of antitrust violations" until it filed its administrative action.[229] According to the court, until the commencement of an administrative action, the FTC investigation had merely sought to determine *whether* the policyholder had committed antitrust violations.[230] Thus, the *ProMedica* court held that there was no coverage under the policy until the FTC

---

documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf ("Regulatory Action" within definition of "Claim" includes "a request for information, civil investigative demand or civil proceeding brought by or on behalf of a governmental agency, including requests for information related thereto").

224. *See* Hertz Glob. Holdings, Inc. v. Nat'l Union Fire Ins. Co., No. 19-CV-06957 (AJN), 2021 WL 1198802, at *6–8 (S.D.N.Y. Mar. 30, 2021) (denying coverage for costs associated with an SEC investigation because (1) the investigation was not an administrative or regulatory proceeding, and therefore did not meet the definition of "securities claims," and (2) although the policy covered investigations against covered individuals, the insured failed to sufficiently allege that the investigation was against individuals).

225. Emp'rs' Fire Ins. Co. v. ProMedica Health Sys., Inc., 524 F. App'x 241 (6th Cir. 2013).

226. Note that the insurer in *ProMedica* had denied coverage on the basis that the policyholder's notice was not timely; thus, it was the policyholder, not the insurer, arguing that a "Claim" had not arisen under the policy until the filing of the FTC's administrative proceedings.

227. Emp'rs' Fire Ins. Co. v. ProMedica Health Sys., Inc., 524 F. App'x 241, 243 (6th Cir. 2013).

228. *Id*. at 247.

229. *Id*. at 248.

230. *Id*. at 249.

filed a complaint against the policyholder alleging various antitrust violations.[231]

The requirement of a "Wrongful Act" was considered in the context of a cyber risk policy in *Travelers v. Federal Recovery Services*.[232] In that case, the court held that the insurer had no duty to defend its insured under a technology errors and omissions policy against an underlying suit in which the sole allegations related to intentional conduct.[233] The Travelers policy defined "errors and omissions wrongful act" to mean "any error, omission or negligent act."[234] The court reasoned that the claims—that the insured refused to return its clients' confidential customer billing information—were not because of an "error, omission, or negligent act" as required by the policy, but rather that the insured acted with knowledge, willfulness and malice.[235]

Some cyber policies may eliminate these issues by not including the same kind of requirements for "formal investigation" or specific assertions of a "Wrongful Act" that sometimes exist in certain types of traditional policies. The extent of coverage for regulatory investigations and informal actions, as well as coverage for regulatory remedies and the availability of defense coverage,[236] are important factors in evaluating cyber coverage.

[G] Definition of Loss

Another area raised by regulatory activities is coverage for fines, penalties, and disgorgement. Some policies purport to exclude coverage for fines and penalties or for violations of law.[237] Others explicitly provide such coverage.[238]

---

231. *Id*. at 253.
232. Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., 103 F. Supp. 3d 1297 (D. Utah 2015).
233. *Id*. at 1302.
234. *Id*. at 1299.
235. *Id*.
236. *See supra* notes 249–251 and accompanying text.
237. *See, e.g.*, Mortenson v. Nat'l Union Fire Ins. Co., 249 F.3d 667, 669 (7th Cir. 2001) ("the policy excludes losses consisting of 'fines or penalties imposed by law or other matters'"); Hartford Fire Ins. Co. v. Guide Corp., No. IP 01-572-C-Y/F, 2005 WL 5899840, at *2 (S.D. Ind. Feb. 14, 2005) (policy "contains an exclusion for punitive damages, fines, and penalties"); *see also* Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 957 F. Supp. 2d 1135, 1155–56 (C.D. Cal. 2013) (adopting insurer argument that civil penalties, attorney fees, and disgorgement under California statute are not covered damages under insurance policy), *aff'd*, 635 F. App'x 351 (9th Cir. 2015); *supra* notes 88–91.
238. *See, e.g.*, Taylor v. Lloyd's Underwriters of London, No. CIV.A. 90-1403, 1994 WL 118303, at *7 (E.D. La. Mar. 25, 1994) (contract stated: "Clause (9)

Even where such remedies are covered by the policy language, insurers sometimes argue that the coverage is contrary to public policy. This issue was considered by the Illinois Supreme Court in *Standard Mutual Insurance Co. v. Lay*,[239] where the insurer argued that coverage for statutory damages of $500 per violation under the Telephone Consumer Protection Act (TCPA)[240] should be denied as akin to punitive damages. Some states hold that coverage for punitive damages is contrary to public policy[241] or is allowed only under limited circumstances.[242] After reviewing the relevant statutory history, the court concluded in *Lay* that the statutory damages under the TCPA were compensatory in nature and not precluded by public policy.[243] In an effort to avoid such issues, policies sometimes contain provisions that require the determination of coverage for punitive

---

of the P&I policy actually *extends* coverage for: Liability for fines and penalties . . . ."); CNA Insurance Co., Fiduciary Liability Solutions Policy, GL2131XX (2005) (insurance policy covered a percentage of liability for fines and penalties for violations of ERISA, its English equivalent, and HIPAA requirements).

239. Standard Mut. Ins. Co. v. Lay, 989 N.E.2d 591, 597 (Ill. 2013).

240. *See supra* note 76.

241. *See, e.g.*, Ace Am. Ins. Co. v. Dish Network LLC, 883 F.3d 881, 888 (10th Cir. 2018) ("TCPA's statutory damages are penal under Colorado law and, even if they were otherwise covered under the policies, Colorado's public policy prohibits the insurability of such penalties and bars coverage."); Soto v. State Farm Ins. Co., 635 N.E.2d 1222, 1224 (N.Y. 1994) ("a rule permitting recovery for excess civil judgments attributable to punitive damage awards would be unsound public policy"). *See also* Maritz Holdings Inc. v. Certain Underwriters at Lloyd's London, No. 4:18-CV-00825 SEP, 2020 WL 7023952, at *4 (E.D. Mo. Nov. 30, 2020) (holding that policyholder's vexatious refusal claims could proceed under Missouri law after the insurer refused to cover two data breach incidents despite New York choice-of-law provisions in the insurance agreements because Missouri has a strong interest in protecting its citizens from unfair insurance practices).

242. *See, e.g.*, Magnum Foods, Inc. v. Cont'l Cas. Co., 36 F.3d 1491, 1497–98 (10th Cir. 1994) (holding that insurance coverage of punitive damages is against public policy, except when the party seeking coverage has been held liable for punitive damages solely under vicarious liability).

243. Lay, 989 N.E.2d at 599–602; *see also* Evanston Ins. Co. v. Gene by Gene Ltd., 155 F. Supp. 3d 706, 711 (S.D. Tex. 2016) (holding that the request for actual and statutory damages "falls under the Policies' definition of damages"); Columbia Cas. Co. v. HIAR Holding, LLC, 411 S.W.3d 258, 268 (Mo. 2013) (holding that "TCPA statutory damages of $500 per occurrence are not damages in the nature of fines or penalties"). The Tenth Circuit, however, reached a contrary conclusion in Ace Am. Ins. Co. v. Dish Network, LLC, 883 F.3d 881, 888 (10th Cir. 2018), holding

damages or regulatory remedies to be governed by "favorable law" or by law of a specific jurisdiction such as England or Bermuda, which has case law permitting such coverage.[244]

There also has been active litigation in recent years concerning the availability of insurance for certain regulatory remedies such as disgorgement. In some cases, the issue is dealt with as an issue of public policy with different courts taking different views of the issue. While some cases suggest that disgorgement of ill-gotten gains may not be insurable as a matter of public policy,[245] others come to a different conclusion.[246] These varying decisions may turn on whether

---

that "TCPA's statutory damages are penal under Colorado law and, even if they were otherwise covered under the policies, Colorado's public policy prohibits the insurability of such penalties and bars coverage."

244. *See, e.g.*, Lancashire Cty. Council v. Mun. Mut. Ins. Ltd [1997] QB 897 (Eng.) ("There is no present authority in English law which establishes that it is contrary to public policy for an insured to recover under a contract of insurance in respect of an award of exemplary damages whether imposed in relation to his own conduct or in relation to conduct for which he is merely vicariously liable. Indeed newspapers, we are told, regularly insure against exemplary damages for defamation.").

245. *See, e.g.*, Ryerson Inc. v. Fed. Ins. Co., 676 F.3d 610, 613 (7th Cir. 2012) (describing a policy that covers disgorgement of ill-gotten gains and stating that "no state would enforce such an insurance policy"); Unified W. Grocers, Inc. v. Twin City Fire Ins. Co., 457 F.3d 1106, 1115 (9th Cir. 2006) ("California case law precludes indemnification and reimbursement of claims that seek the restitution of an ill-gotten gain") (citation omitted); Level 3 Commc'ns, Inc. v. Fed. Ins. Co., 272 F.3d 908, 910 (7th Cir. 2001) (district court should have ruled that disgorging profits of theft is against public policy); Mortenson v. Nat'l Union Fire Ins. Co., 249 F.3d 667, 672 (7th Cir. 2001) ("It is strongly arguable, indeed, that insurance against the section 6672(a) penalty, by encouraging the nonpayment of payroll taxes, is against public policy[.]").

246. *See, e.g.*, Genzyme Corp. v. Fed. Ins. Co., 622 F.3d 62, 69 (1st Cir. 2010) ("We see no basis in Massachusetts legislation or precedent for concluding that the settlement payment is uninsurable as a matter of public policy."); Westport Ins. Corp. v. Hanft & Knight, P.C., 523 F. Supp. 2d 444, 453 (M.D. Pa. 2007) (finding an insurer's argument that public policy prohibits coverage for disgorgement "unavailing"); Genesis Ins. Co. v. Crowley, 495 F. Supp. 2d 1110, 1120 (D. Colo. 2007) (court declined to adopt insurer's argument that disgorgement is uninsurable as a matter of public policy); BLaST Intermediate Unit 17 v. CNA Ins. Cos., 674 A.2d 687, 689–90 (Pa. 1996) (finding that coverage for disgorgement of ill-gotten gains did not violate public policy); Astellas US Holding, Inc. v. Starr Indem. & Liab. Co., 566 F. Supp. 3d 879, 906 (N.D. Ill. 2021) ("[T]here is in fact no general Illinois public policy prohibiting insurance for damages caused by the insured's intentional acts, unless the insured wrongdoing is the one to recover the proceeds.").

there is a true disgorgement of profits, the regulator is a pass-through, or disgorgement is a surrogate measure of damages.[247]

Public policy arguments aside, the language of the policy can be important. For example, some courts have found disgorgement to fall within the meaning of "loss," while others have found that it does not fall within the meaning of "damages."[248] Depending on policy wording, defense costs may be covered with respect to a disgorgement claim even where a court holds that public policy precludes indemnity coverage.[249] Similarly, an insurer may be obligated to pay defense costs even though a regulatory remedy may not be covered, as long as the regulatory proceeding constitutes a claim under the applicable policy definition.[250] Finally, as noted above, policies sometimes contain specific choice-of-law provisions requiring application of the law of a jurisdiction that favors coverage for remedies like fines or penalties.[251]

---

247. *See, e.g.*, Limelight Prods., Inc. v. Limelite Studios, Inc., 60 F.3d 767, 769 (11th Cir. 1995) ("recognizes ill-gotten profits as merely another form of damages that the statute permits to be presumed because of the proof unavailability in these actions"); JP Morgan Sec., Inc. v. Vigilant Ins. Co., 37 N.Y.3d 552, 568–69 (2021) (reversing Appellate Division decision and finding that component of SEC disgorgement settlement payment intended to compensate harmed investors was covered loss and not a "penalty imposed by law" under broker dealer professional liability policy). *See also* Liu v. Sec. & Exch. Comm'n, 140 S. Ct. 1936, 1949–50 (2020) (holding that disgorgement awards in SEC actions may not exceed the gains made "when both the receipts and payments are taken into account").

248. *Compare* Chubb Custom Ins. Co. v. Grange Mut. Cas. Co., No. 2:07-cv-1285, 2011 U.S. Dist. LEXIS 111583, at *31 (S.D. Ohio Sept. 29, 2011) (a policy's definition of loss covered wrongfully retained money), *with* Cont'l Cas. Co. v. Duckson, 826 F. Supp. 2d 1086, 1097 (N.D. Ill. 2011) ("return of profits obtained illegally does not constitute covered damages"); *see also* Level 3 Commc'ns, Inc. v. Fed. Ins. Co., 272 F.3d 908, 910 (7th Cir. 2001) (noting that policies covering "damages" provide broader coverage than those insuring against a "loss").

249. *See, e.g.*, Vigilant Ins. Co. v. Credit Suisse First Bos. Corp., No. 600854/2002, 2003 WL 24009803, at *5 (N.Y. Sup. Ct. July 8, 2003) (finding that because the "term 'loss' includes defense costs," insurer must pay for them, even though the remedy for disgorgement of ill-gotten gains is not insurable as a matter of public policy).

250. *See, e.g.*, Bodell v. Walbrook Ins. Co., 119 F.3d 1411, 1414 (9th Cir. 1997) (holding that an insurer must pay defense costs related to a U.S. Postal Inspection Service investigation as the regulatory proceeding constituted a claim under the policy, even though a remedy for fraud would not be covered).

251. *See* text accompanying *supra* note 244.

[H] Who Controls Defense and Settlement

The issue of who controls the selection of counsel, the course of defense, and decisions whether to settle can be extremely important under any insurance policy. Many policies, including cyber policies, give the insurer varying degrees of control over these issues. These matters should be considered at the time a policy is being negotiated, when there may be flexibility on both sides, as opposed to after a claim arises.

With respect to the selection of counsel, insurance policies that contain a duty to defend often give the insurance company the unilateral right to appoint counsel unless there is a reservation of rights or some other situation that gives the insured the right to appoint counsel at the insurer's expense.[252] Policyholders are sometimes surprised to find that they are confronted with a case that is very important to them but that their policy allows attorneys or other professionals to be selected and controlled in varying degrees by the insurer.[253] While this may not be a policyholder concern in routine matters without significant reputational or other exposure to the company, or in situations where there is a service that has been bargained and paid for by the insured, insureds confronted with a cyber breach may prefer to select and utilize their own counsel.

A compromise position in some policy forms involves the use of "panel counsel." Under this approach, the policyholder is entitled to select counsel for the defense of a claim, but choices are restricted to a list of lawyers designated by the insurer. In some cases, the

---

252. *Compare* Twin City Fire Ins. Co. v. Ben Arnold-Sunbelt Beverage Co., 433 F.3d 365, 367 (4th Cir. 2005) ("The insurance company, in turn, typically chooses, retains, and pays private counsel to represent the insured as to all claims."), *with* HK Sys., Inc. v. Admiral Ins. Co., No. 03 C 0795, 2005 WL 1563340, at *16 (E.D. Wis. June 27, 2005) (when there is a conflict of interest between the insurer and the insured, "the insurer retains the right either to choose independent counsel or to allow the insured to choose counsel at the insurer's expense"), San Diego Navy Fed. Credit Union v. Cumis Ins. Soc'y, 208 Cal. Rptr. 494, 506 (Ct. App. 1984) ("[T]he insurer must pay the reasonable cost for hiring independent counsel by the insured . . . [and] may not compel the insured to surrender control of the litigation."), *superseded by* CAL. CIV. CODE § 2860 (2012), *and* Md. Cas. Co. v. Peppers, 355 N.E.2d 24, 31 (Ill. 1976) (insured "has the right to be defended in . . . case by an attorney of his own choice" that is paid for by insurer, when there is a conflict between insurer and insured).

253. The ethical obligations of counsel in these circumstances can be particularly complex. *See, e.g.*, WILLIAM T. BARKER & CHARLES SILVER, PROFESSIONAL RESPONSIBILITIES OF INSURANCE DEFENSE COUNSEL §§ 11–12, 14 (2017).

list is appended to the policy. In others, it is set forth on a website maintained by the insurer.[254] In either case, the policyholder may be contractually limited to selecting counsel from the panel counsel list, at least in the absence of a conflict of interest.[255]

The panel counsel lists of most major insurance companies include well-known and able lawyers; however, there can be concerns about the panel counsel approach from the insured's perspective. First, panel counsel often expect to receive an ongoing flow and volume of work from the insurance company. As a result, they may be overly attentive to the insurance company's approach and the way in which it wants to handle cases. Second, in some cases, panel counsel have agreed to handle cases for a particular insurance company's insureds at discounted rates. These rate requirements may preclude law firms with substantial expertise in a particular area from agreeing to participate on the panel. Low rates may also incentivize use of less experienced lawyers. Third, panel counsel are not necessarily lawyers typically used by the policyholder. As a result, they may have no familiarity with the policyholder or its business and management and may lack the trust built by a long attorney-client relationship.

In light of these concerns, it is important to review panel counsel provisions in a particular policy. In many cases where a policyholder has a "go-to" counsel that it expects to use in the event of a covered claim, the insurance company will agree in advance to include those lawyers on the panel counsel list for that particular insured. This is an issue that should be considered when the policy is being negotiated since it is frequently easier to negotiate inclusion of a policyholder's normal counsel before the policy is issued, as opposed to after a claim has occurred.

The issue of selection of counsel is closely aligned to the questions of control of defense and control of settlement. Particularly where there is a duty to defend, the insurer may have a high degree of control of the defense of a claim. While disagreements between the insurer and the insured on defense strategy may raise difficult legal and ethical issues,[256] the key for present purposes is, again, to

---

254. *See, e.g.*, Panel Counsel Directory, AIG, www-191.aig.com/#/dashboard; *Approved EPL Panel Counsel Defense Firms*, CHUBB, www2.chubb.com/us-en/business-insurance/approved-epl-panel-counsel-defense-firms.aspx.

255. *See, e.g.*, Md. Cas. Co. v. Peppers, 355 N.E.2d 24, 31 (Ill. 1976) (entitled to independent counsel where insured could be held liable on either negligent or intentional claims and only negligent act claims were covered under policy); CAL. CIV. CODE § 2860 (2018) (codifies independent counsel requirement in San Diego Navy Fed. Credit Union v. Cumis Ins. Soc'y, Inc., 162 Cal. App. 3d 358 (Ct. App. 1984)).

256. *See, e.g.*, N. Cty. Mut. Ins. Co. v. Davalos, 140 S.W.3d 685, 689 (Tex. 2004) ("Every disagreement [between insurer and insured] about

consider the matter when the policy is being negotiated so the parties understand the implications of the policy being purchased. At a minimum, the insured will almost always have a duty to cooperate with its insurer that raises issues about privilege and other matters.[257] In addition, policies often include insurer rights to consent to settlement and to covered expenditures that should be reviewed both when a policy is negotiated and in the event of a claim.[258]

---

how the defense should be conducted cannot amount to a conflict of interest . . . . If it did, the insured, not the insurer, could control the defense by merely disagreeing with the insurer's proposed actions."). *See generally* WILLIAM T. BARKER & CHARLES SILVER, PROFESSIONAL RESPONSIBILITIES OF INSURANCE DEFENSE COUNSEL §§ 11–12, 14 (2017); 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 17.07 (2020) (discussing the consequences an insurer's breach of the duty to defend).

257. *See, e.g.*, Martinez v. Infinity Ins. Co., 714 F. Supp. 2d 1057, 1062–63 (C.D. Cal. 2010) (insurance policy at issue imposed upon the insured a duty to cooperate to hand over privileged financial documents to the insurer); Kimberly-Clark Corp. v. Cont'l Cas. Co., No. 3-v5-cv-0475-D, 2006 U.S. Dist. LEXIS 63576, at *5 (N.D. Tex. Aug. 18, 2006) ("attorney-client communications or attorney work product . . . are not abrogated by the cooperation clause"); Remington Arms Co. v. Liberty Mut. Ins. Co., 142 F.R.D. 408, 416 (D. Del. 1992) (even when an insured has a duty to cooperate with insurer, "insurance coverage actions did not foreclose the assertion of attorney-client privilege"); Purze v. Am. All. Ins. Co., 781 F. Supp. 1289, 1292–93 (N.D. Ill. 1991) (the duty to cooperate in the insurance contract at issue involved insured giving insurer banking information); Waste Mgmt., Inc. v. Int'l Surplus Lines Ins. Co., 579 N.E.2d 322, 327–28 (Ill. 1991) ("condition in the policy requiring cooperation on the part of the insured is one of great importance . . . . A fair reading of the terms of the contract renders any expectation of attorney-client privilege, under these circumstances, unreasonable."). *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 16.04 (2020).

258. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § XIV.C (2009), www.chubb.com/businesses/csi/chubb10308.pdf ("No Insured shall settle or offer to settle any Claim . . . without the Company's prior written consent"); PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § I.C (2010), www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form31-932.pdf ("Extortion expenses and extortion monies shall not be paid without prior consultation with us and with our express written consent. You must make every reasonable effort to notify the local law enforcement authorities; and notify the Federal Bureau of Investigation or similar equivalent foreign agency, before surrendering any extortion monies in response to an extortion demand"); TRAVELERS, CyberRisk Form CYB-3001, § II.V. (ed. 07-10), www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-3001.pdf ("E-Commerce Extortion Expenses means any Money or Securities the Insured Organization pays, with the Company's [Insurer's] prior written

These issues may be particularly significant in the context of settlements and ransom demands. Most policies give an insurer the right to consent to any settlement, although courts differ as to whether the insurer must be prejudiced in order to defeat coverage.[259] In some cases, a policyholder may want to settle and the insurer may believe the amount proposed is excessive. In certain circumstances, the insurer can refuse to consent,[260] but must generally act reasonably[261] and may face liability in excess of policy limits if the insured is later required to pay a judgment in excess of the proposed settlement.[262]

Alternatively, the insurer may want to settle where the policyholder does not. Some insurance policies give the insurer the right to

---

consent and pursuant to a recommendation by an Approved Service Provider, at the direction and demand of any person committing or allegedly committing E-Commerce Extortion.").

259. *Compare* Booking v. Gen. Star Mgmt. Co., 254 F.3d 414, 421 (2d Cir. 2001) ("[A] breach of a 'settlement-without-consent' clause is material only if it prejudices the insurer.") (applying Texas law) *and* Progressive Direct Ins. Co. v. Jungkans, 972 N.E.2d 807, 811 (Ill. App. Ct. 2012) ("[A]n insurer who invokes a cooperation clause must affirmatively show that it was prejudiced by the insured's failure to notify it in advance of his settlement with the tortfeasor"), *with* Benecard Servs., Inc. v. Allied World Specialty Ins. Co., No. 20-2359, 2021 WL 4077047, at *1–2 (3d Cir. Sept. 8, 2021) (insurer did not need to show prejudice to deny coverage where insured settled without consent because the "consent clause is a clear term of [the policy]") (applying New Jersey law).

260. *See, e.g.*, Certain Underwriters of Lloyd's v. Gen. Accident Ins. Co. of Am., 909 F.2d 228, 232 (7th Cir. 1990) (an insurer may refuse to settle, as "the insurer has full control over defense of the claim, including the decision to settle"); RESTATEMENT OF THE LAW OF LIABILITY INSURANCE § 25 (2019).

261. *See, e.g.*, RESTATEMENT OF THE LAW OF LIABILITY INSURANCE §§ 24–25 and comments thereto (2019).

262. *See, e.g.*, Am. Hardware Mut. Ins. Co. v. Harley Davidson of Trenton, Inc., 124 F. App'x 107, 112 (3d Cir. 2005) ("The *Rova Farms* rule is thus: (1) if a jury could find liability, (2) where the verdict could exceed the policy limit, and (3) the third-party claimant is willing to settle within the policy limit, then (4) in order to be deemed to have acted in good faith, the insurer must initiate settlement negotiations and exhibit good faith in those negotiations. American Hardware was obligated to initiate settlement negotiations and did not; therefore it acted in bad faith and is liable for the excess verdict."); Nat'l Union Fire Ins. Co. v. Cont'l Ill. Corp., 673 F. Supp. 267, 270 (N.D. Ill. 1987) ("Illinois has long recognized an insured's right to hold the insurer responsible for an amount in excess of the policy limits when the insurer has been guilty of fraud, bad faith or negligence in refusing to settle the underlying claim against the insured within those limits."); RESTATEMENT OF THE LAW OF LIABILITY INSURANCE § 25 (2019).

do this, while other policies do not.[263] Others provide that where an insurer wants to settle and an insured does not, only a specified percentage of future fees and settlement costs in excess of the rejected settlement will be covered.[264] Again, the starting place is the policy, so the language should be considered by the parties at the time the policy is being negotiated.

[I] Control of Public Relations and Crisis Management Professionals

Many cyber policies provide coverage for certain kinds of crisis management activities, which may encompass expenses of public relations experts and certain kinds of advertising.[265] This issue can be especially important to the extent cyber policies give insurers

---

263. *Compare* Sec. Ins. Co. v. Schipporeit, Inc., 69 F.3d 1377, 1383 (7th Cir. 1995) (policy required the insured's consent to a settlement), *and* Brion v. Vigilant Ins. Co., 651 S.W.2d 183, 184 (Mo. Ct. App. 1983) (terms of the policy required the insured's consent), *with* Papudesu v. Med. Malpractice Joint Underwriting Ass'n of R.I., 18 A.3d 495, 498–99 (R.I. 2011) (insurance policy gave the insurer the right to settle "as it deems expedient," even without insured's consent).

264. *See, e.g.*, Chubb, CyberSecurity Form 14-02-14874, § XIV.D (2009), www.chubb.com/businesses/csi/chubb10308.pdf ("If any Insured withholds consent to any settlement acceptable to the claimant . . . then the Company's liability for all Loss, including Defense Costs, from such Claim shall not exceed the amount of the Proposed Settlement plus Defense Costs incurred[.]"); AIG CyberEdge Security and Privacy Liability Insurance, Form 101024 (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf ("The Insurer's duty to defend ends if an Insured refuses to consent to a settlement that the Insurer recommends. . . and that the claimant will accept. As a consequence of such Insured's refusal, the Insurer's liability shall not exceed the amount for which the Insurer could have settled such Claim had such Insured consented, plus Defense Costs incurred prior to the date of such refusal, plus 50% of Defense Costs incurred with the Insurer's prior written consent after the date of such refusal.").

265. *See, e.g.*, Chubb, CyberSecurity Form 14-02-14874, § I.C. (2009), www.chubb.com/businesses/csi/chubb10308.pdf (providing coverage for crisis management expenses, which includes advertising and public relations media and activities); AIG CyberEdge Security and Privacy Liability Insurance, Form 101024 (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf ("Loss" includes costs incurred within one year of discovery of security failure or security event for "a public relations firm, crisis management firm or law firm agreed to by the Insurer to advise an Insured on minimizing the harm to such Insured, including, without limitation, maintaining and restoring public confidence in such Insured.").

control of negotiation and payment in actual or threatened ransomware or cyber extortion attacks.[266]

In some cases, the dollar limits for crisis management and public relations are relatively low and these coverages may cede control of experts and budget, in varying degrees, to the insurer. Media experts who deal with cyber privacy breaches often have special expertise, and some policyholders view insurer expertise in selecting the right experts and managing these kinds of situations as one of the benefits of purchasing coverage. Other policyholders may not wish to relinquish control of these issues, particularly where limits applicable to crisis management expenses are small. In some cases, the policyholder may deal with these matters by negotiating with the insurer to include the policyholder's chosen expert as an option under the policy. In any event, selection and management of public relations and crisis management professionals, like selection of defense attorneys, is a consideration that should be evaluated by the insurer and policyholder in negotiating cyber coverages.

[J] Issues Created by Involvement of Policyholder Employees

Some policies exclude "loss caused by an employee."[267] This kind of exclusion can be problematic in a cyber policy where cyber events sometimes involve an inside job.[268]

Even where there is not a blanket employee exclusion, insurance policies often preclude coverage for liabilities expected or intended or damage knowingly caused by "the insured."[269] A common question

---

266. TRAVELERS, CyberRisk Form CYB-3001, § II.V. (ed. 07-10), www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-3001.pdf ("E-Commerce Extortion Expenses means any Money or Securities the Insured Organization pays, with the Company's [Insurer's] prior written consent and pursuant to a recommendation by an Approved Service Provider, at the direction and demand of any person committing or allegedly committing E-Commerce Extortion.")

267. *See, e.g.*, CNA NetProtect 360, Form G-147051-A, § VI.A.1; Chubb Executive Protection Portfolio, Crime Insurance Policy—Retail, Form 14-02-7307, § 13(b) (2010).

268. *See supra* notes 156–159 and accompanying text regarding employee involvement issues under crime policies.

269. *See, e.g.*, Everest Nat'l Ins. Co. v. Valley Flooring Specialties, No. CV F 08-1695 LJO GSA, 2009 U.S. Dist. LEXIS 36757, at *19 (E.D. Cal. Apr. 14, 2009) ("intentional and knowing conduct exclusions unambiguously apply"); Auto Club Grp. Ins. Co. v. Marzonie, 527 N.W.2d 760, 768 n.23 (Mich. 1994) (policy precluded coverage for injury that was intended or activity that "the actor knew or should have known" would

in insurance contracts, which may be significant under cyber policies, is whose knowledge controls the applicability of potentially applicable exclusions.

The obvious concern in the cyber context is the situation in which an employee is intentionally responsible for a security breach or perhaps for selling confidential information to others. Resultant claims against the employee are likely excluded, in varying degrees, by most insurance policies. But the question that arises is whether any applicable exclusions are limited to the responsible employee or the corporate policyholder as a whole.

Case law developed under traditional insurance coverages varies with respect to the extent to which knowledge or intentional misconduct by an employee can be attributed to the policyholder for purposes of denying coverage. Some cases require the knowledge to be by a senior person or officer or director before the intent will be attributed to the company.[270] Others may not.[271]

Today, many policies deal with this issue by use of a severability clause. A typical such clause states that no fact pertaining to, and no knowledge possessed by, any insured person shall be imputed to another insured person, and many specify that only the knowledge of certain high-level company officers is imputed to the company.[272]

---

cause injury), *abrogated by* Frankenmuth Mut. Ins. Co. v. Masters, 595 N.W.2d 832 (Mich. 1999). *See generally* 3 ALLAN WINDT, INSURANCE CLAIMS AND DISPUTES § 11:9 (6th ed. Updated Online Mar. 2022).

270. *See, e.g.*, Legg Mason Wood Walker, Inc. v. Ins. Co. of N. Am., No. 78-0927, 1980 U.S. Dist. LEXIS 13088, at *18 (D.D.C. July 24, 1980) (because neither of individuals involved in intentional misconduct was an officer, director, stockholder, or partner, the insured's claim is still covered by insurer).

271. *See, e.g.*, FMC Corp. v. Plaisted & Cos., 72 Cal. Rptr. 2d 467, 61 Cal. App. 4th 1132, 1212–13 (Ct. App. 1998) (upholding jury instructions that stated "[K]nowledge which a corporation's employee receives or has in mind when acting in the course of his or her employment is in law the knowledge of the corporation, if such knowledge concerns a matter within the scope of the employee's duties."), *overruled on other grounds by* California v. Cont'l Ins. Co., 281 P.3d 1000 (Cal. 2012).

272. *See, e.g.*, Chubb, CyberSecurity Form 14-02-14874, § IV (2009), www.chubb.com/businesses/csi/chubb10308.pdf ("for the purposes of determining the applicability of [certain exclusions] . . . A. no fact pertaining to or knowledge possessed by any Insured Person shall be imputed to any other Insured Person to determine if coverage is available; and B. only facts pertaining to or knowledge possessed by an Insured Organization's [certain executive officers] shall be imputed to such Insured Organization to determine if coverage is available"). *See generally* 4 JEFFREY E. THOMAS, APPLEMAN ON INSURANCE § 26.07 (2020).

Under such clauses, the knowledge or intent is limited to the relevant individual and not attributed to others.[273]

A second issue with these kinds of exclusions arises when knowledge or intent is disputed. While some policies limit the ability of an insurer to deny coverage in this context to situations where there has been a "final adjudication," the courts vary on whether such an adjudication must be in an underlying case or can be in an insurance coverage case, including one initiated by the carrier.[274] Insurance policies often address this issue by utilization of a final adjudication clause. An illustrative policy provision provides:

> The company shall not be liable under Insuring Clause X for Loss on account of any Claim made against any Insured Person:
>
> (a) based upon, arising from, or in consequence of any deliberately fraudulent act or omission or any willful violation of any statute or regulation by such Insured Person, if a *final, non-appealable adjudication in any underlying proceeding or action* establishes such a deliberately fraudulent act or omission or willful violation; or
>
> (b) based upon, arising from, or in consequence of such Insured Person having gained any profit, remuneration or other advantage to which such Insured Person was not legally entitled, if a *final, non-appealable adjudication in any underlying proceeding or action* establishes the gaining of such a profit, remuneration or advantage.[275]

---

273. *See, e.g.*, Chrysler Ins. Co. v. Greenspoint Dodge of Houston, Inc., 297 S.W.3d 248, 253 (Tex. 2009) (stating, in the context of a severability clause, "intent and knowledge for purposes of coverage are determined from the standpoint of the particular insured, uninfluenced by the knowledge of any additional insured").

274. *See, e.g.*, Wintermute v. Kan. Bankers Sur. Co., 630 F.3d 1063, 1071–73 (8th Cir. 2011) (insurer not relieved of duty to defend based on personal profit and dishonesty exclusions unless proven in underlying case that the director actually received personal gain or was involved in dishonest acts); Pendergest-Holt v. Certain Underwriters at Lloyd's of London, 600 F.3d 562, 573 (5th Cir. 2010) ("in fact" language is read more broadly than a "final adjudication" clause and satisfied by a final judgment in either the underlying case or a separate coverage case); Atl. Permanent Fed. Sav. & Loan Ass'n v. Am. Cas. Co., 839 F.2d 212 (4th Cir. 1988) (the exclusion does not apply unless there is a judgment adverse to the officers and directors in the underlying suit); *see also infra* notes 275–277.

275. *See, e.g.*, Chubb Primary Directors & Officers and Entity Securities Liability Insurance Policy Form 14-02-18480 (2017), www.chubb.com/us-en/_assets/doc/14-02-18480-primary-policy.pdf (emphasis added).

Note that the specific reference to "underlying proceeding" in this particular clause is designed to require adjudication in the underlying case.[276] These kinds of provisions may be construed to require defense and indemnity in the absence of a final adjudication so that the insured is entitled to coverage in the event of a settlement where there has never been an actual adjudication of wrongdoing.[277]

The final adjudication language can also be an important protection for policyholders in social engineering cases in which the employee is an unwitting vehicle for the loss, rather than a culpable accomplice.[278] For example, the Ninth Circuit upheld an insurer's denial of coverage under a company's crime policy on the basis of an employee's "involvement" in a social engineering scheme in which the fraudster convinced the employee that certain payments should be routed to a new bank account.[279] By the time it was discovered that those payments had been rerouted improperly, more than $700,000 had been lost.[280] Coverage was denied because the policy excluded coverage for losses resulting from the input of data by authorized employees and the employee who changed the deposit information was authorized to enter such data.[281] The employee's unwitting involvement therefore defeated coverage. Final adjudication language may have prevented loss of coverage because the involvement of the authorized employee was innocent.

Another type of exclusion involving company employees seeks to preclude coverage for failure to consistently implement cyber risk controls.[282] These kinds of exclusions can be vetted and tied to

---

276. *See generally* Dan A. Bailey, *D&O Policy Commentary*, *in* INSURANCE COVERAGE 2004: CLAIM TRENDS & LITIGATION, at 205, 215 (PLI Litig. & Admin. Practice, Course Handbook Ser. No. 702, 2004) (when a D&O policy requires "final adjudication" in the underlying action to trigger an exclusion, courts have held that the adjudication must occur in the underlying proceeding and not in a parallel coverage action).

277. *See, e.g.*, Atl. Permanent Fed. Sav. & Loan Ass'n v. Am. Cas. Co. of Reading, Pa., 839 F.2d 212, 216–17 (4th Cir. 1988) (the exclusion does not apply unless there is a final judgment adverse to the officers and directors in the underlying suit).

278. *See supra* notes 156–159 and *infra* notes 291–292 and accompanying text.

279. Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., 719 F. App'x 701, 702 (9th Cir. 2018).

280. Appellant's Opening Br., Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. 16-35614 (Dkt. 11), at 3–6 (9th Cir. Dec. 9, 2016).

281. Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., 719 F. App'x 701, 702 (9th Cir. 2018).

282. *See, e.g.*, Complaint, Columbia Cas. Co. v. Cottage Health Sys., No. 15-cv-03432 (C.D. Cal. May 7, 2015) (excluding "[a]ny failure of an Insured to continuously implement the procedures and risk controls

specific company policies and procedures to avoid subsequent differences as to what is a relevant procedure and what is not.

[K] Coverage of a *Threatened* Security Breach—Ransomware

Most insurance policies cover actual loss or damage.[283] The usual CGL policy, for example, covers bodily injury, property damage, and personal and advertising injury. Property damage policies typically cover direct physical damage.[284] While some property damage policies also cover costs to avoid certain harm to physical property,[285] that may not encompass a security breach, much less a threatened security breach or "ransomware attack."[286] Cyber policies or ransomware

---

identified in the Insured's application . . . and all related information submitted to the Insurer"); Star Title Partners of Palm Harbor, LLC v. Ill. Union Ins. Co., No. 8:20-CV-2155-JSM-AAS, 2021 WL 4509211, at *4–5 (M.D. Fla. Sept. 1, 2021) (no coverage for fraudulent email prompting wire transfer because, *inter alia*, authenticity of email was not "verified in accordance with [Insured's] internal procedures" as required under definition of "Deceptive Transfer Fraud").

283. *See, e.g.*, QBE Ins. Corp. v. ADJO Contracting Corp., 934 N.Y.S.2d 36 (Sup. Ct. 2011) ("A policy is implicated when the insured learns of an actual loss or injury covered by the policy, and not when the insured learns only of a potentially dangerous condition.") (citing Chama Holding Corp. v. Generali-US Branch, 22 A.D.3d 443, 444–45 (N.Y. App. Div. 2005)). *But see* Baughman v. U.S. Liab. Ins. Co., 662 F. Supp. 2d 386, 393 (D.N.J. 2009) ("court-ordered medical monitoring with costs to be paid by defendants . . . is 'damages' under [the policy]," even though not actual damage).

284. *See, e.g.*, Wash. Mut. Bank v. Commonwealth Ins. Co., No. 56396-3-I, 2006 Wash. App. LEXIS 1316, at *6–7 (Ct. App. June 26, 2006) (holding that plain language of property damage policy required "direct physical loss of or damage to insured property").

285. *Id*. at *11.

286. A ransomware attack involves electronic files being held hostage until a ransom is paid. These attacks are becoming increasingly common. One attack in May 2017, called "WannaCry," involved attacks on hundreds of thousands of companies, including National Health Service organizations in the United Kingdom. Alexander Smith, Saphora Smith, Nick Bailey & Petra Cahill, *Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.*, NBC NEWS (May 17, 2017), www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126. Another ransomware attack in December 2021 on Ultimate Kronos Group, a workforce management solutions company, disrupted cloud-based time entry, scheduling, and payroll processing for thousands of employers. Michelle Shen, *Ransomware attack on Kronos could disrupt how companies pay, manage employees for weeks*, USA TODAY (Dec. 14, 2021), https://finance.yahoo.com/news/ransomware-attack-takes-down-hr-223356146.html. In the entertainment industry,

endorsements typically deal with this risk explicitly by covering the cost to respond to a threatened cyber attack, including conducting a follow-up investigation.[287] In some cases, business interruption losses may also be covered,[288] though it is important to consider applicable

---

movies and television shows like *Pirates of the Caribbean 5* and *Orange is the New Black* have been subject to ransomware attacks. Daniel Bukszpan, *Disney Hacking Shows Why Companies Shouldn't Succumb to Digital Blackmail, Experts Say*, CNBC NEWS (May 21, 2017), www.cnbc.com/2017/05/21/disney-hacking-shows-why-companies-shouldnt-succumb-to-digital-blackmail-experts-say.html. Ransomware attacks against governments have also become increasingly common; Atlanta, Georgia; Baltimore, Maryland; and Riveria Beach, Florida have all been attacked recently. Patricia Mazzei, *Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000*, N.Y. TIMES (June 19, 2019), www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html; Nicole Perlroth & Scott Shane, *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html. The state of Louisiana declared a state of emergency twice in 2019 due to ransomware attacks. The city of New Orleans similarly issued an emergency warning after it experienced its own attacks. Kate Fazzini, *New Orleans Shuts Off Computers After Cyberattack, Following Two Big Incidents in Louisiana this Year*, CNBC (Dec. 13, 2019), www.cnbc.com/2019/12/13/new-orleans-reports-cyberattacks-after-other-attacks-in-louisiana.html. Employees of America's largest companies and major news organization who are working from home are reportedly being targeted by a Russian ransomware group in retaliation against the U.S. government. David E. Sanger & Nicole Perlroth, *Russian Criminal Group Finds New Target: Americans Working at Home*, N.Y. TIMES (June 25, 2020), www.nytimes.com/2020/06/25/us/politics/russia-ransomware-coronavirus-work-home.html.

287. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § I.G (2009), www.chubb.com/businesses/csi/chubb10308.pdf ("The Company shall pay E-Threat Expenses resulting directly from an Insured having surrendered any funds or property to a natural person who makes a Threat directly to an Insured during the Policy Period."); PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § I.C (2010), www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form31-932.pdf ("We will reimburse you for the extortion expenses and extortion monies . . . paid by you and resulting directly from any credible threat or series of credible threats.").

288. ALLIANZ GLOBAL CORPORATE & SPECIALTY, A GUIDE TO CYBER RISK: MANAGING THE IMPACT OF INCREASING INTERCONNECTIVITY 19–20 (2015), www.agcs.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html#; MARSH, MANAGING OPERATIONAL RISKS: PRIVACY AND COMPUTER SECURITY PROTECTION FOR CYBER CATASTROPHE PLACEMENTS 3 (2015), www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Cyber%20CAT%20(Fact%20Sheet).pdf.

limits and sublimits since downtime from a ransomware attack is often quite short. It is important to review a cyber policy to determine whether threats, as opposed to only actual damage, are covered. Coverage may also be sought for down-time or computer shutdown in response to a threatened breach. Policy language can also be considered to determine if the policy covers only threats to extort money or other kinds of threats as well.

[L] Coverage for "Breachless" Claims

In addition to actual and threatened breaches, companies increasingly face litigation[289] and regulatory claims[290] alleging that the company or its products are merely *susceptible* to a data breach. For example, in a 2015 putative class action in California, plaintiff car owners sued several car manufacturers alleging that the hacking of the computers in their cars was an "imminent eventuality," though there was no evidence their "vehicles [had] actually been hacked, or that they [were] aware of any vehicles that have been hacked outside of controlled environments."[291] Similarly, two putative class

---

289. *See, e.g.*, Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955 (N.D. Cal. 2015); Complaint, Ross v. St. Jude Med., Inc., No. 16-6506 (C.D. Cal. Aug. 26, 2016), *dismissed without prejudice*, Ross v. St. Jude Med., Inc., No. 2:16-CV-06465 (C.D. Cal. Dec. 28, 2016), ECF No. 11; Complaint, Shore v. Johnson & Bell, Ltd., No. 16-cv-04363 (N.D. Ill. Apr. 15, 2016), Defendant's Motion to Direct Plaintiff to Proceed to Arbitration on an Individual Basis and Enjoin Class Arbitration Granted, Shore v. Johnson & Bell, Ltd., No. 1:16-CV-04363 (N.D. Ill. Feb. 22, 2017), ECF No. 65.

290. Complaint at 5–6, FTC v. D-Link Corp., No. 17-cv-00039 (N.D. Cal. Jan. 5, 2017) (alleging that manufacturer's wireless routers and Internet cameras were *susceptible* to a breach despite there being no allegations of an actual cyber attack against the company's products), *dismissed*, No. 17-cv-00039 (N.D. Cal. Aug. 6, 2019), ECF No. 276 (parties settled and agreed to a stipulated order for injunction); Opinion at 17, *In re* LabMD, Inc., No. 9357 (FTC July 29, 2016) (holding that a showing of tangible injury was not necessary in order for company acts and practices to be considered unfair), www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf, *vacated sub nom.* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1231 (11th Cir. 2018) (holding unenforceable the FTC's cease and desist order for LabMD to implement security measures, "assum[ing] *arguendo* that the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice").

291. *Cahen*, 147 F. Supp. 3d at 958–59 (dismissing complaint for lack of standing "given the lack of injury flowing from the asserted potential hacking issue"); Flynn v. FCA US LLC, 39 F.4th 946, 949–50 (7th Cir.

actions were brought in 2016—one against an implantable cardiac device manufacturer, in which patients alleged their devices could be hacked,[292] and another against a law firm alleging that client data was at risk of being stolen due to the firm's insufficient security measures.[293] Notably, none of the plaintiffs in these cases alleged that a cyber event had actually occurred.[294]

Such "breachless" claims present difficult insurance issues. Some cyber policies require an actual breach to trigger coverage for third-party liability claims.[295] While certain policies contain language that triggers first-party coverage (for example, for an investigation or notification costs) based on a "reasonably suspected" incident,[296] the types of suits described above may arguably fall outside the "reasonably suspected" language since those breachless claims only allege the danger of a breach, as opposed to one that is believed to have occurred.

2022) (dismissing for lack of standing a consumer class action alleging Jeep Cherokees were vulnerable to hacking because plaintiffs could not prove an actual injury).

292. Complaint, Ross v. St. Jude Med., Inc., No. 16-6506 (C.D. Cal. Aug. 26, 2016) (alleging that St. Jude Medical and related companies failed to protect implantable cardiac devices from potential hackers), *dismissed without prejudice*, Ross v. St. Jude Med., Inc., No. 2:16-CV-06465 (C.D. Cal. Dec. 28, 2016), ECF No. 11.

293. Complaint, Shore v. Johnson & Bell, Ltd., No. 16-cv-4363 (N.D. Ill. Apr. 15, 2016), Defendant's Motion to Direct Plaintiff to Proceed to Arbitration on an Individual Basis and Enjoin Class Arbitration Granted, Shore v. Johnson & Bell, Ltd., No. 1:16-CV-04363 (N.D. Ill. Feb. 22, 2017), ECF No. 65.

294. *But see* Complaint, Wengui v. Clark Hill, PLC, No. 19-cv-03195 (D.D.C. Feb. 2, 2020); Order Granting Motion for Protective Order, Wengui v. Clark Hill, PLC, No. 19-cv-03195 (D.D.C. May 26, 2020) (hackers allegedly gained access to the firm's computer system and published the client's information on the Internet); Complaint, Kan. City. Hiscox Ins. Co. v. Warden Grier, Dkt. No. 4:20-cv-00237-NKL (E.D. Mo. Mar. 27, 2020) (alleging that law firm breached its legal and ethical obligations by failing to protect client confidences and client data from hackers who gained access to the firm's systems and stole client data).

295. *See, e.g.*, CNA NetProtect 360, Form G-147051-A, § X, Privacy Injury (defining a "Privacy Injury" to include the "failure of Insured Entity to prevent unauthorized access to, unauthorized disclosure of, or unauthorized use of Confidential Commercial Information").

296. *See, e.g.*, ALPS Cyber Risk and Security Breach Liability Insurance Policy, Form ALPS Cyber (06-13), § I.B (providing coverage for Privacy Breach Response Services if there is a cyber incident "or reasonably suspected incident").

[M] The "Internet of Things" and Potential Physical Damage or Bodily Injury from a Cyber Attack

With the ever-increasing "Internet of Things" (IoT) (everyday physical objects like cars, garage doors, and refrigerators that are connected to the Internet),[297] the availability of devices prone to cyber attacks continues to grow on a daily basis.[298] One report projects there will be 27 billion devices connected to the Internet by 2025, up from 12.2 billion in 2021.[299] The spectrum of IoT devices that are vulnerable to attack range from consumer goods[300] to medical devices[301] and include industrial, government, and commercial applications.[302]

---

297. *Internet of Things (IoT)*, TECHOPEDIA, www.techopedia.com/definition/28247/internet-of-things-iot ("The internet of things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices.").

298. *See, e.g.*, Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955 (N.D. Cal. 2015) (computers in automobiles alleged to be susceptible to hacking).

299. Mohammad Hasan, *State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally*, IOT ANALYTICS (May 18, 2022), https://iot-analytics.com/number-connected-iot-devices/#:~:text=The%20forecast%20for%20the%20total,30.9%20billion%20forecasted%20in%202020).

300. *See, e.g.*, Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 M. Vehicles for Bug Fix*, WIRED (July 24, 2015), www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/ (discussing how a hacker could take over the steering, transmission, or brakes of an Internet-accessible car); Flynn v. FCA US LLC, 39 F.4th 946, 949–50 (7th Cir. 2022) (dismissing consumer class action alleging Jeep Cherokees were vulnerable to hacking because plaintiffs could not prove an actual injury). *See also* Complaint at 5, FTC v. D-Link Corp., No. 17-cv-00039 (N.D. Cal. Jan. 5, 2017) (alleging that an Internet camera and wireless router manufacturer failed to take adequate security measures to protect its devices), *dismissed*, No. 17-cv-00039 (N.D. Cal. Aug. 6, 2019), ECF No. 276 (parties settled and agreed to a stipulated order for injunction). In the FTC's first children's privacy and security case, VTech Electronics settled a claim by the FTC alleging that the toymaker's Internet-connected products collected personal information about children without providing notice and obtaining parental consent, and thereafter failed to adequately protect the information it collected. United States v. VTech Elecs., Ltd., No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018). *See also supra* note 198.

301. *See, e.g.*, Complaint, Ross v. St. Jude Med., Inc., No. 16-6506 (C.D. Cal. Aug. 26, 2016) (alleging that defendant and related companies failed to protect implantable cardiac devices from potential hackers), *dismissed without prejudice*, Ross v. St. Jude Med., Inc., No. 2:16-CV-06465 (C.D. Cal. Dec. 28, 2016), ECF No. 11.

302. *See, e.g.*, LLOYD'S EMERGING RISK REPORT 2015, BUSINESS BLACKOUT: THE INSURANCE IMPLICATIONS OF A CYBER ATTACK ON THE US POWER

A necessary consequence of this increasingly interconnected world is a growing threat of physical damage caused by cyber attack. A hacker attack on a manufacturer's operating system could cause a severe breakdown in equipment.[303] While few such incidents have been widely reported,[304] they are no longer restricted to science fiction or the movies. For example, as motor vehicles become increasingly reliant on technology and, indeed, become driverless, the opportunities for hackers to cause a car to act erratically and cause physical damage or bodily injury also increases. Increasing interconnectedness further exacerbates the risk.[305]

GRID (2015), https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf (describing the severe implications of a hypothetical attack on a "smart" power grid, resulting in a widespread blackout across the Northeast, leaving millions without power and shutting down phone systems, Internet, television, traffic signals, factories and commercial activity for several days); *see also Business Blackout*, LLOYD'S (July 6, 2015), www.lloyds.com/businessblackout; WHAT EVERY CISO NEEDS TO KNOW ABOUT CYBER INSURANCE, at 2 (Symantec White Paper 2015) ("Experts are telling us we could experience a massive cyber terrorist event that could cause major market disruptions, and even physical damage to property and critical infrastructure."), www.symantec.com/content/dam/symantec/docs/white-papers/what-every-ciso-needs-to-know-cyber-insurance-en.pdf.

303. *See, e.g.*, Lucy L. Thomson, *Cyber Physical Risk*, 2016 ABA Litig. Sec. Ins. Coverage Litig. Committee 7–12 (discussing attacks ranging from the disabling of a computer system designed to detect pipeline leaks (which caused a major oil spill and loss of life) to a hacking incident causing four trains to derail).

304. In one widely reported incident, Colonial Pipeline Co. was the victim of a ransomware attack that led the company to temporarily shut down a pipeline that supplies nearly half the gasoline, diesel, and jet fuel used on the U.S. East Coast. Colonial paid the $4.4 million ransom demanded by the hackers and filed an insurance claim to help cover the loss. Ben Kochman, *Colonial Seeks Insurance Payout for $4.4M Cyberattack*, LAW360 (June 9, 2021), www.law360.com/articles/1392096/colonial-seeks-insurance-payout-for-4-4m-cyberattack.

305. *See generally* Nathan Bomey, *Uber Self-Driving Car Crash: Vehicle Detected Arizona Pedestrian 6 Seconds Before Accident*, USA TODAY (May 24, 2018), www.usatoday.com/story/money/cars/2018/05/24/uber-self-driving-car-crash-ntsb-investigation/640123002/; Jack Stewart, *Why Tesla's Autopilot Can't See a Stopped Firetruck*, WIRED (Jan. 25, 2018), www.wired.com/story/tesla-autopilot-why-crash-radar/; Cybersecurity in automotive: Mastering the challenge (Mar. 2020), MCKINSEY & CO., www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/cybersecurity%20in%20automotive%20mastering%20the%20challenge/cybersecurity-in-automotive-mastering-the-challenge.pdf.

This growing threat of physical damage may be difficult to insure. On one hand, traditional coverages increasingly include cyber-related exclusions, like the 2004 ISO endorsement excluding "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[306] On the other hand, cyber policies often exclude third-party liability coverage for bodily injury and property damage.[307]

In order to deal with these risks, some cyber insurers now offer enhanced coverage to include coverage for the physical loss or third-party property damage or bodily injury that arise from a cyber attack.[308] Another option for filling this potential gap in coverage may be cyber difference-in-conditions (DIC) coverage, which is now offered by several insurers and generally provides coverage for perils excluded under other policies.[309] Alternatively, a carefully crafted technology errors and omissions policy could provide coverage in the event an insured's IoT-enabled component is hacked and causes

---

306. *See, e.g.*, Jeff Woodward, *The 2004 ISO CGL Policy*, INT'L RISK MGMT. INST. (Apr. 2004), www.irmi.com/articles/expert-commentary/the-2004-iso-cgl-policy; *see also* Institute Cyber Attack Exclusion Clause (CL 380) (Oct. 11, 2003) ("in no case shall this insurance cover loss, damage, liability, or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system"); *see supra* note 46 and accompanying text.

307. *See, e.g.*, AIG, Specialty Risk Protector, CyberEdge Security and Privacy Liability Insurance, Security and Privacy Coverage Section, § 3(d) (Dec. 2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf ("This policy shall not cover Loss in connection with a Claim made against an Insured . . . alleging, arising out of, based upon or attributable to any Bodily Injury or Property Damage.").

308. *See, e.g.*, AIG, *CyberEdge Plus* (2016), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-plus-070616-final-digital.pdf; Marsh's Cyber CAT 4.0 is advertised as offering coverage for third-party property damage and bodily injury liability caused by a cyber event, www.marsh.com/us/services/cyber-risk.html.

309. *See, e.g.*, *Cyber Coverage & Services*, AEGIS (offering a difference-in-conditions option "which wraps coverage around existing policies, i.e., property, casualty, terrorism and environmental" and "delivers full cyber coverage for physical damage, bodily injury and environmental issues"), www.aegislink.com/aegislink/services/underwriting/products/cyber-coverage-and-services.html; AIG CyberEdge PC (Apr. 2014 (offering umbrella difference-in-conditions coverage for, inter alia, property damage)), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-pc-product-profile-final.pdf.

damage to a customer's larger product or system, or, worse, to a consumer.[310]

Policyholders and insurers should work closely with information technology professionals, brokers, risk managers, and attorneys to review their existing scope of coverages and the potential need for insurance for cyber-related physical damage or bodily injury.[311]

[N] Governmental Activity Exclusion

Cyber policies may include provisions limiting coverage for government-sponsored activities. Traditional policies often limit coverage for war and acts of terrorism and, even where they cover terrorist activity by individuals or political groups, policies may exclude coverage for acts of government or government-sponsored organizations.[312] This may be particularly problematic in the cyber context where cyberspace has been deemed a warfare "domain" by the U.S. government.[313] Numerous reports have discussed the allegations of government-sponsored hacking by China, North Korea, Russia, Iran, and other countries into U.S. government agencies and major corporations.[314] In April 2021, the U.S. government imposed

---

310. *Technology Errors and Omissions Insurance (Tech E&O)*, INT'L RISK MGMT. INST., www.irmi.com/online/insurance-glossary/terms/t/technology-errors-and-omissions-insurance-tech-eo.aspx ("Tech E&O policies cover both liability and property loss exposures.").

311. *See, e.g.*, Tony Martucci, *How Automakers Can Minimize Cybersecurity Liability*, LAW360 (June 15, 2021), www.law360.com/california/articles/1394766?utm_source=shared-articles&utm_medium=email&utm_campaign=shared-articles.

312. *See* Merck & Co., Inc. v. Ace Am. Ins. Co., No. UNN-L-002682-18, 2022 WL 951154, (N.J. Super. Jan. 13, 2022) (granting summary judgment that "Hostile/Warlike Action" exclusion does not apply to the 2017 NotPetya ransomware attack, whether or not the attack was instigated by Russia to harm Ukraine, because the plain meaning of "hostile or warlike action" encompasses traditional physical action, such as use of armed forces, not "cyber" attacks, of which the parties were aware but did not expressly exclude). In another case, the insured filed suit seeking coverage under its first-party property insurance for damage to its servers and laptops caused by the "NotPetya" malware attack, for which the insurer allegedly denied coverage under the policy's exclusion for governmental, hostile or warlike action. Complaint, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018). *See also* note 286 discussing ransomware attacks.

313. Jim Garamone, *Cybercom Chief Discusses Importance of Cyber Operations*, U.S. DEP'T OF DEFENSE (Apr. 14, 2015), www.defense.gov/News/News-Stories/Article/Article/604453/cybercom-chief-discusses-importance-of-cyber-operations/.

314. Michael R. Gordon, Vivian Salama & Anna Hirtenstein, *U.S. Puts Fresh Sanctions on Russia Over Hacking, Election Interference*, WALL ST. J.

sanctions on Russia and expelled ten Russian diplomats for its participation in the Solar Winds cyber attack and attempts to impact the 2020 presidential election.[315] China has also been accused of breaching corporate Microsoft Exchange email systems to conduct espionage.[316]

The complexities posed by these circumstances are illustrated by the decision of the U.S. Court of Appeals for the Ninth Circuit in *Universal Cable Productions, LLC v. Atlantic Specialty Insurance Co.*[317] In that case, Universal concluded that it could no longer guaranty the safety of the Jerusalem production set for its television series *Dig* after "Hamas fired rockets from Gaza into Israel" and engaged in a number of other "hostilities."[318] When Universal sought coverage for the significant expenses it incurred in moving the set out of Jerusalem, the insurer, Atlantic Specialty, denied coverage.[319] While Atlantic Specialty recognized that the imminent threat of injury triggered coverage under its television production insurance policy, and that its policy covered "terrorism," it took the position that coverage was excluded under exclusions for:

1. *War*, including undeclared or civil war; or
2. *Warlike action* by a military force, including action in hindering or defending against an actual or expected attack, by

---

(Apr. 15, 2021), www.wsj.com/articles/biden-signs-executive-order-targeting-harmful-foreign-activities-by-russian-government-11618490399; Zolan Kano-Youngs & David E. Sanger, *U.S. Accuses China of Hacking Microsoft*, N.Y. TIMES (July 20, 2021), www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html; Ben Kochman, *Google Says Likely N. Korean Hackers Targeted Security Pros*, LAW360 (Apr. 1, 2021), www.law360.com/articles/1370994/google-says-likely-n-korean-hackers-targeted-security-pros; Nicole Pelroth, *Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies*, N.Y. TIMES (Feb. 18, 2019), www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.

315. Ellen Nakashima, *Biden administration imposes significant economic sanctions on Russia over cyberspying, efforts to influence presidential election*, WASH. POST (Apr. 15, 2021), www.washingtonpost.com/national-security/biden-to-announce-tough-sanctions-on-russia-over-cyber-spying/2021/04/15/a4c1d260-746e-11eb-948d-19472e683521_story.html.

316. Zolan Kano-Youngs & David E. Sanger, *U.S. Accuses China of Hacking Microsoft*, N.Y. TIMES (July 20, 2021), www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html.

317. Universal Cable Prods., LLC v. Atl. Specialty Ins. Co., 929 F.3d 1143 (9th Cir. 2019), *reh'g and reh'g en banc denied* (Sept. 4, 2019).

318. *Id*. at 1147, 1150.

319. *Id*. at 1147–48.

> any government, sovereign, or other authority using military personnel or other agents.[320]

Applying a provision of the California Insurance Code that required adherence to terms with technical or trade usage meanings,[321] the court concluded that "war" and "warlike action" had special meanings in the insurance context, of which the parties were presumed aware, and required the action of a "de facto or de jure sovereign."[322] After a careful analysis of the role of Hamas in the Middle East,[323] the court concluded that Hamas did not satisfy this requirement and that the two exclusions at issue did not apply.[324]

While not all jurisdictions have a legislated counterpart to the statutory provision at issue in the *Universal Cable* case, some have case law giving weight to industry usage.[325] Regardless of whether that is the case, *Universal Cable* illustrates the complex factual issues about the nature of a particular hacker which may arise where war or terrorism exclusions are asserted in response to a cyber attack, as well as the importance of careful legal review and analysis when war and terrorism exclusions are being negotiated into a cyber policy. Recent renewals of cyber and other coverages have involved

---

320. *Id*. at 1149 (emphasis in original). Atlantic Specialty also denied coverage under a third exclusion: "3. Insurrection, rebellion, revolution, usurped power, or action taken by the governmental authority in hindering or defending against any of these. Such loss or damage is excluded regardless of any other cause or event contributed concurrently or in any sequence to the loss." *Id*. However, the court determined that exclusion presented factual issues which it remanded for consideration by the district court. *Id*. at 1161–62. The court did not apply the doctrine of contra preferendum, which typically requires any ambiguity in an exclusion to be construed against the insurer, particularly where it drafted the policy, both because of the asserted sophistication of Universal and the insurer and the involvement of both the insurer and the policyholder, through its broker, in preparing the policy. *Id*. at 1152–53.

321. *Id*. at 1153 (quoting CAL. CIV. CODE § 1644: terms in an insurance policy are to be "understood in their ordinary and popular sense, rather than according to their strict legal meaning; unless used by the parties in a technical sense, or unless a special meaning is given to them by usage, in which case the latter must be followed.").

322. Universal Cable, 929 F.3d at 1154–55 (citing Pan Am World Airways v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1012 (2d Cir. 1974); Holiday Inns, Inc. v. Aetna Ins. Co., 571 F. Supp. 1460 (S.D.N.Y. 1983); 10A COUCH ON INSURANCE § 152:3 (3d ed. Updated Online June 2022)).

323. Universal Cable, 929 F.3d at 1147–48.

324. *Id*. at 1155–61.

325. *See generally* Allan D. Windt, INSURANCE CLAIMS AND DISPUTES § 6:2 (6th ed. Updated Online Mar. 2022).

negotiation of new war and terrorism exclusions drafted by insurers in response to events in Ukraine.[326]

[O] Other Exclusions

Cyber policies often contain important exclusions that substantially narrow coverage. For example, some cyber policies exclude damage to computers and related business interruption on the theory that these risks should be covered by a more traditional property policy, at least when due to natural causes.[327] Cyber policies may also exclude securities claims,[328] but a cyber breach involving confidential financial information may be among a company's most important securities risks. Employment claims are also excluded under certain cyber policies, though the disclosure of confidential information about employees is an important risk for many companies.[329] Antitrust exclusions may be at issue where information is stolen or disclosed for anticompetitive purposes. In addition, cyber policies often contain a fraud exclusion, though

---

326. Daphne Zhang, *Russia War Raises Global Insurers' Cyber Claim Exposure*, LAW360 (Mar. 11, 2022), www.law360.com/articles/1471913/russia-war-raises-global-insurers-cyber-claim-exposure; Daphne Zhang, *Willis Says Insurers Adding Exclusions for Ukraine War*, LAW360 (Apr. 11, 2022), www.law360.com/articles/1483046?scroll=1&related=1; Judy Greenwald, *Lloyd's requiring state-backed cyberattack exclusions*, BUS. INS. (Aug. 18, 2022), www.businessinsurance.com/article/20220818/NEWS06/912351890/Lloyd%E2%80%99s-requiring-state-backed-cyber attack-exclusions.

327. *See, e.g.*, PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § IV.C (2010), www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form31-932.pdf (excluding from loss expenses that arise out of "fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption . . . or any other physical event or peril"); *see also* Chubb, CyberSecurity Form 14-02-14874, § III.C.6 (2009), www.chubb.com/businesses/csi/chubb10308.pdf (excluding from loss any expense "resulting from mechanical failure, faulty construction, error in design, latent defect, wear or tear, gradual deterioration").

328. *See, e.g.*, PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § IV.R (2010), www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form31-932.pdf (excluding from coverage violations of the Securities Exchange Act).

329. *See* PHILA. INS. CO., Cyber Security Liability Coverage Form PI-CYB-001, § IV.L (2010), www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form31-932.pdf (excluding from coverage employment practices or discrimination claims). See also employment-related practices exclusions considered in the BIPA context, discussed at *supra* notes 99–100.

many cyber attacks include at least some element of fraudulent misconduct.[330]

Another important exclusion may concern business interruption. Some policies specifically exclude business interruption due to a cyber event. Others specifically provide that coverage.[331] The potential impact of cyber losses on an insured's ability to conduct business should be carefully evaluated by the parties to determine whether coverage for this kind of business interruption loss is necessary or appropriate. Particular attention should be given to limits and sublimits since outages from cyber claims are sometimes brief but can cause significant loss of income and extra expense.

Exclusions for liability assumed under contract or agreement are also increasingly important in the cyber context,[332] as illustrated by the court decision denying P.F. Chang's' claim under a cyber policy.[333]

---

330. *See, e.g.*, First Bank of Del., Inc. v. Fid. & Deposit Co. of Md., No. N11C-08-221 MMJ CCLD, 2013 WL 5858794, at *9 (Del. Sup. Ct. Oct. 30, 2013) (finding insurance for a data breach under D&O policy's "electronic risk liability" coverage, which covered "any unauthorized use of, or unauthorized access to electronic data or software with a computer system," reasoning that every unauthorized use or access would almost necessarily involve fraud and thus a fraud exclusion would render coverage illusory); G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 89 (Ind. 2021) (defining "fraudulently cause a transfer" to mean "to obtain by trick" and denying summary judgment for both parties because not all ransomware attacks that "hijack" the policyholders' computer system are "necessarily fraudulent").

331. *See, e.g.*, Travelers Cyber Risk Form CYB-3001, § I.J (2010) ("The Company will pay the Insured Organization for Business Interruption Loss incurred by the Insured Organization which is directly caused by a Computer System Disruption taking place during the Policy Period[.]"); Complaint, Moses Afonso Ryan Ltd. v. Sentinel Ins. Co., No. 1:17-CV-00157 (D.R.I. Apr. 21, 2017) (a small law firm was extorted of $25,000 by a ransomware attack and suffered a multiple-month business interruption resulting in more than $700,000 in damages, and was denied coverage under its property policy), Stipulation of Dismissal with Prejudice Ordered, Moses Afonso Ryan Ltd. v. Sentinel Ins. Co., No. 1:17-CV-00157 (D.R.I. May 1, 2018), ECF No. 16.

332. *See, e.g.*, Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233 (5th Cir. 2018); St. Paul Fire & Marine Ins. Co. v. Rosen Millennium Inc., No. 6:17-CV-540-ORL-41-GJK (M.D. Fla. Mar. 27, 2017), *decided on other grounds*, St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., 337 F. Supp. 3d 1176 (M.D. Fla. 2018); P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016), *appeal dismissed*, No. 16-16141 (9th Cir. Jan. 27, 2017), ECF No. 15.

333. P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016), *appeal dismissed*, No. 16-16141 (9th Cir. Jan. 27, 2017), ECF No. 15.

The case involved a data breach in which thousands of customers' credit card numbers were allegedly compromised.[334] The insurer covered certain costs of a forensic investigation into the data breach and the costs of defending litigation filed by third parties whose credit card information was stolen; however, it denied coverage for amounts the insured owed to its credit card servicer under their master service agreement (MSA), which included:

(1) reimbursement of fraudulent charges on the stolen credit cards;

(2) costs to notify cardholders and to reissue new cards to affected individuals; and

(3) a flat fee relating to P.F. Chang's compliance with Payment Card Industry Data Security Standards (PCI DSS).[335]

In addition to holding that the fees to the credit card servicer did not trigger coverage under the policy's definition of a "Privacy Injury,"[336] the court held that coverage was barred under two exclusions precluding coverage for contractual obligations assumed by the insured.[337] The court cited the MSA between the insured and its credit card servicer, which required the insured to reimburse the servicer for fees the servicer incurred (for example, reimbursement of fraudulent charges and notification costs).[338] Some courts have reached similar conclusions, while others have not.[339]

---

334. *Id*. at *1–2.

335. *Id*.

336. *Id*. at *4–5. The court held that there was no "Privacy Injury," because that term was defined as "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record, or exceeding access to such Person's Record." *Id*. at *4. Since the lost credit card information belonged to the customers' themselves—not the credit card servicer that brought suit against P.F. Chang's—the court concluded there was no injury sustained by a Person because of unauthorized to "*such* Person's record." *Id*.

337. *Id*. at *7–8.

338. *Id*. at *8.

339. *See, e.g.*, Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233 (5th Cir. 2018); St. Paul Fire & Marine Ins. Co. v. Rosen Millennium Inc., No. 6:17-CV-540-ORL-41-GJK (M.D. Fla. Mar. 27, 2017), *decided on other grounds*, St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., 337 F. Supp. 3d 1176 (M.D. Fla. 2018). *But see* Landry's, Inc. v. Ins. Co. of the State of Pennsylvania, 4 F.4th 366 (5th Cir. 2021) (finding that injuries from publication of customers' credit card information arose from violation of privacy rights "as those terms are commonly understood," regardless of legal theories that sounded in contract); Target Corp. v. Ace Am. Ins. Co., No. 19-CV-2916 (WMW/DTS), 2022 WL 848095,

Credit card arrangements are often covered by specific provisions in cyber policies. Insureds that process credit card transactions as a part of their business should give particular attention to these provisions and should consider cyber policies that explicitly include this coverage.[340] In addition, any contractual liability exclusion, like that involved in the *P.F. Chang's* case, should be reviewed to determine whether it applies to PCI-DSS assessments levied pursuant to an MSA or other agreement.[341]

Some policies also contain exclusions that preclude coverage if the policyholder fails to continuously maintain risk controls identified in its application for insurance.[342] Such provisions should be reviewed by insurance and technical personnel at insurers and policyholders when the policy is negotiated and subsequently by the policyholder to ensure continuing compliance.

---

at *3 (D. Minn. Mar. 22, 2022) (holding CGL policy covers settlement Target paid to banks that reissued customer credit cards following data breach for "loss of use" because "[a]lthough the compromised cards still existed . . . they could no longer serve their function").

340. *See, e.g.*, AIG, Specialty Risk Protector, CyberEdge Security and Privacy Liability Insurance, Security and Privacy Coverage Section, § 2(h), 3(j) (2013) (defining "Loss" to include "amounts payable in connection with a PCI-DSS Assessment," which is in turn is defined as "any written demand received by an Insured from a Payment Card Association . . . or bank processing payment card transactions . . . for a monetary assessment (including a contractual fine or penalty) in connection with an Insured's non-compliance with PCI Data Security Standards which resulted in a Security Failure or Privacy Event"), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf.

341. *See, e.g.*, AIG, Specialty Risk Protector, CyberEdge Security and Privacy Liability Insurance, Security and Privacy Coverage Section, § 3(j)(9) (2013), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf (excluding "amounts an Insured agrees to pay pursuant to a contract, including without limitation, liquidated damages, setoffs or penalties; *provided, however, this exclusion shall not apply to any PCI-DSS Assessment*") (emphasis added).

342. Minute Order, Cottage Health v. Columbia Cas. Co., No. 16CV02310 (Sup. Ct. Cal. Santa Barbara Cty. Oct. 13, 2017) (noting that dispute stems, in part, from policyholders' alleged failure to "continuously implement the risk controls it identified in its policy application"); *see also* note 282; Star Title Partners of Palm Harbor, LLC v. Ill. Union Ins. Co., No. 8:20-CV-2155-JSM-AAS, 2021 WL 4509211, at *4–5 (M.D. Fla. Sept. 1, 2021) (no coverage for fraudulent email prompting wire transfer because, *inter alia*, authenticity of email was not "verified in accordance with [Insured's] internal procedures" as required under definition of "Deceptive Transfer Fraud").

§ 16:3.3 SEC Disclosure and Other Regulatory Initiatives

The importance of insurance for cyber risks, and an understanding of such insurance, is underscored by SEC guidance and enforcement actions. For more than a decade, SEC guidance has required publicly traded companies to disclose, among other things:

- risk factors relating to a potential cyber incident, including known or threatened attacks;
- costs and other consequences associated with known cyber incidents or risks of potential incidents;
- material legal proceedings involving cyber incidents; and
- insurance for cyber risks.[343]

The SEC has also proposed new rules regarding cybersecurity disclosures that expand on previous rules and would require periodic reporting regarding cybersecurity policies and procedures to identify risks, the role of the board of directors and management in overseeing and implementing cybersecurity controls, and disclosure of any director's cybersecurity expertise.[344] These requirements emphasize the need for cyber insurance and a clear understanding of what such policies cover. The filing of two SEC administrative actions[345] confirms that failure to make disclosures of cyber risks, incidents, policies, and protections could potentially subject registrants to SEC enforcement action[346] and shareholder

---

343. *CF Disclosure Guidance: Topic No. 2, Cybersecurity, U.S. Sec. & Exch. Comm'n* (Oct. 13, 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

344. *See* SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, U.S. SEC. & EXCH. COMM'N (Mar. 9, 2022), www.sec.gov/news/press-release/2022-39.

345. *In re* Person PLC (Aug. 16, 2021) (resulting in $1 million civil penalty), www.sec.gov/litigation/admin/2021/33-10963.pdf; *In re* First Am. Fin. Corp. (June 14, 2021) (resulting in cease and desist order and nearly $500,000 civil penalty), www.sec.gov/litigation/admin/2021/34-92176.pdf. The SEC also appears to be investigating whether companies failed to make the necessary disclosures regarding the effects of the SolarWinds cyber attack on their businesses. *See In re* Certain Cybersecurity-Related Events (June 24, 2021) (commencing an investigation into the SolarWinds cyber attack and sending a letter requesting certain entities provide information on a voluntary basis), www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

346. *See* John Reed Stark, *SEC Cyber Disclosure Actions Point to Merciless Scrutiny*, LAW360 (Aug. 24, 2021), www.law360.com/assetmanagement/

suits.[347] Additional SEC guidance expands on the types of insurance-related disclosures that should be made.[348]

Numerous government and regulatory authorities at the state[349] and federal levels in the United States, in the European Union,[350] and in other countries,[351] most recently China,[352] have been extremely

---

articles/1415344?utm_source=shared-articles&utm_medium=email&utm_campaign=shared-articles.

347. *See supra* section 16:2.3[A].

348. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, U.S. Sec. & Exch. Comm'n (Feb. 26, 2018), www.sec.gov/rules/interp/2018/33-10459.pdf.

349. Michael Bahar et al., *An Emerging Patchwork of Cybersecurity Rules*, LAW360 (Aug. 29, 2017), www.law360.com/articles/957355/an-emerging-patchwork-of-cybersecurity-rules; Allison Grande, *NY Cybersecurity Rules will be Enforced as they Mature*, LAW360 (Feb. 14, 2018), www.law360.com/articles/1012620/ny-cybersecurity-rules-will-be-enforced-as-they-mature; Lawrence Hamilton et al., *Dissecting NAIC's Insurance Data Security Model Law*, LAW360 (Oct. 24, 2017), www.law360.com/articles/988848/dissecting-naic-s-insurance-data-security-model-law. Statement of Charges, *In re* First Am. Title Ins. Co., No. 2020-0030-C (July 21, 2020), www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf (New York's Department of Financial Regulation filed charges against First American Title Insurance Company for allegedly violating the state's Cybersecurity Requirements for Financial Services Companies by failing to properly test and remedy a website vulnerability that allowed unprotected access to tens of millions of records containing consumers' sensitive data).

350. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1 (GDPR became effective on May 25, 2018, and deals with processing the personally identifiable information of individuals residing in the European Union, regardless of where a company is located).

351. *See, e.g.*, Law No. 25326, Personal Data Protection Law, Oct. 4. 2000 (Arg.); Constitución Politica de Los Estados Unidos Mexicanos [C.P.], art. 16, www.juridicas.unam.mx/infjur/leg/constmex/pdf/consting.pdf.

352. *See, e.g.*, Personal Information Protection Law of the People's Republic of China (PIPL) (中华人民共和国个人信息保护法) (promulgated by the Standing Committee of the National People's Congress of China, Aug. 20, 2021, effective Nov. 1, 2021), www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (Chinese version); The Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法) (promulgated by the Standing Committee of the National People's Congress of China, Nov. 7, 2016, effective June 1, 2017), www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (Chinese version).

active in dealing with cybersecurity and privacy issues.[353] These kinds of efforts and subsequent regulatory involvement will continue to raise issues with respect to insurance coverage for resultant compliance and investigative costs, as well as private civil liability. For example, California recently enacted the California Consumer Privacy Act (CCPA), which gives individuals more control over how their personal information is handled or shared,[354] and Illinois,

---

353. *See, e.g.*, Michael Nadeau, *General Data Protection Regulation (GDPR) Requirements, Deadlines and Facts*, CSO (June 29, 2017), www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html; European Commission Press Release, Questions and Answers—Data Protection Reform Package (May 24, 2017), http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm; William Shaw, *6 Concerns for Insurance Lawyers as GDPR Approaches*, LAW360 (Jan. 29, 2018), www.law360.com/articles/1006033/6-concerns-for-insurance-lawyers-as-gdpr-approaches; Romaine Marshall & Matt Sorensen, *New NY Cybersecurity Regs Will Have National Reach*, LAW360 (Mar. 22, 2017), www.law360.com/articles/903712/new-ny-cybersecurity-regs-will-have-national-reach; *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NAT'L INST. OF STANDARDS & TECH. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; *Assessments: Cyber Resilience Review (CRR)*, U.S. COMPUTER EMERGENCY READINESS TEAM [US-CERT], www.us-cert.gov/ccubedvp/assessments; U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT (Nov. 2012), www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.

354. *See* CAL. CIV. CODE § 1798.100–1798.199. The CCPA was passed in June 2018 and went into effect January 1, 2020. The statute is designed to establish broad privacy rights for consumers including the rights to know what data is being collected, how that data is being used, and whether the data is being sold or distributed, and to request that personal information be deleted by businesses. *Id*. Along with these rights, the CCPA also grants a limited private right of action when "nonencrypted and nonredacted personal information" is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures." *Id*. § 1798.150(a) (as amended by Assembly Bill 1355 (effective Oct. 11, 2019)). In November 2020, California approved a more comprehensive version of the CCPA updating and modifying certain rules and stipulations to increase the rights of California consumers. The new statute, the California Consumer Privacy Rights Act (CPRA), will go into effect January 1, 2023. *See* CAL. CIV. CODE § 1798.100–1798.199 (amended Nov. 3, 2020, by initiative Proposition 24, effective Dec. 16, 2020, operative Jan. 1, 2023). Virginia, Colorado, Utah, and Connecticut have also enacted comprehensive data privacy laws. *See* 2021 H.B. 2307/2021 S.B. 1392 (Consumer Data Protection Act or CDPA); COLO. REV. STAT. § 6-1-1301 *et seq*. (2021 HS.B. 190) (Colorado Privacy Act or CPA);

Texas, and Washington state have implemented laws regulating biometric data, with the Illinois statute including a private right of action.[355]

UTAH CODE ANN. § 13-61-101 *et seq.* (2022 S.B. 227) (Utah Consumer Privacy Act); S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022) (Connecticut Data Privacy Act or CTDPA).

355. *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2020); WASH. REV. CODE ANN. § 19.375 (West 2020); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2020). The U.S. Senate had introduced a federal National Biometric Information Privacy Act bill, the National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020), which did not pass. The House of Representatives has since introduced a new comprehensive federal privacy law, the American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. (2021–2022).