

7-1-2018

The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses

Erik S. Knutsen

Jeffrey W. Stempel

Follow this and additional works at: <https://elibrary.law.psu.edu/pslr>

Recommended Citation

Knutsen, Erik S. and Stempel, Jeffrey W. (2018) "The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses," *Penn State Law Review*. Vol. 122: Iss. 3, Article 4.

Available at: <https://elibrary.law.psu.edu/pslr/vol122/iss3/4>

This Article is brought to you for free and open access by the Law Reviews and Journals at Penn State Law eLibrary. It has been accepted for inclusion in Penn State Law Review by an authorized editor of Penn State Law eLibrary. For more information, please contact ram6023@psu.edu.

The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses

Erik S. Knutsen and Jeffrey W. Stempel*

ABSTRACT

Insurers currently constrict coverage for losses involving electronic information in traditional insurance product lines. As a result, insurance customers are driven to the brave new world of non-standardized varieties of cyber-risk insurance policies. That world abounds with coverage gaps as the market for cyber insurance sorts itself out. Until that synchronization of coverage for cyber losses occurs, litigation is bound to occur as the boundaries of coverage remain patchwork and uncertain.

This article examines the degree to which cyber losses differ from other insured losses. The cyber-loss insurance coverage jurisprudence reveals a mishmash of principles and coverage terms that are largely focused on the technology of the loss and not on the nature of the loss insured. Unpredictable and unhelpful analogies have ensued, prompting a highly inefficient coverage marketplace and resulting litigation experience. This article also draws parallels with the market experience of a number of now-commonplace insurance coverage products, like commercial general liability policies, that also went through an initial period of uncertainty. Lessons from those prior insurance experiences are instructive as the wild world of cyber insurance stabilizes.

This article proposes that, to reduce the prevalence of insurance coverage disputes about cyber losses, courts should jettison the “cyber” loss differentiation altogether and instead focus on the nature of the inherent risk insured against, as opposed to the risk’s “cyber” quality. Taking a technologically neutral stance—applying “techno-neutrality” to insurance policy language—can act as a market stabilizer. This approach

* Respectively, Professor of Law, Queens University-Canada and Doris S. & Theodore B. Lee Professor of Law, William S. Boyd School of Law, University of Nevada Las Vegas. Special thanks to Chris French and to the *Penn State Law Review* for organizing the symposium from which this paper emanates. Thanks also to Dan Hamilton, Ann McGinley, and Randy Maniloff.

is preferable to introducing new, untested insurance products or, alternatively, risking arbitrary coverage gaps under traditional product lines. The long-term, more commercially sensible solution is for insurers to simply fold cyber-loss coverage into traditional coverage products and not differentiate losses based on particular or peculiar property characteristics.

Table of Contents

I.	INTRODUCTION	646
II.	THE COVERAGE LANDSCAPE FOR CYBER LOSSES	648
III.	THE PHYSICAL-DIGITAL CONUNDRUM FOR CYBER LOSSES	652
IV.	PUBLICATION AND ACCESS HURDLES TO COVERAGE FOR THE RELEASE OF PRIVATE DIGITAL DATA.....	660
V.	THE MARKET SEGMENTATION NIGHTMARE IN A BRAVE NEW COVERAGE WORLD	662
VI.	THE REACTIONARY APPROACH TO “CYBER” ANYTHING	668
VII.	THE INTERIM SOLUTION: A TECHNO-NEUTRAL APPROACH TO POLICY INTERPRETATION	673

I. INTRODUCTION

Insurers currently constrict coverage for losses involving electronic information (hereinafter “cyber losses”) in traditional insurance product lines such as commercial general liability (CGL) and property insurance policies. As a result, insurance customers (i.e., policyholders or prospective policyholders) are driven to the brave new world of non-standardized varieties of cyber-risk insurance policies. That world abounds with coverage gaps as the market for cyber insurance sorts itself out. Until that synchronization of coverage for cyber losses occurs, litigation is bound to occur as the boundaries of coverage remain patchwork and uncertain.

This article proposes that, until the market for cyber-loss coverage stabilizes, the medium- to long-term solution for coverage disputes among insurers and policyholders is to jettison the “cyber” loss differentiation altogether and instead focus on the nature of the inherent risk insured against, as opposed to the risk’s inherent “cyber” quality. Taking a technologically neutral stance, or applying “techno-neutrality” to insurance policy language, may act as a greater market stabilizer than introducing new, untested insurance products or, alternatively, risking arbitrary coverage gaps under traditional product lines. The legal notions of “property” and physicality are changing. No longer is a physical and tangible component necessary to consider something “property.”

If one instead approached cyber losses in a technologically neutral fashion and focused on traditional bedrock insurance principles of risk and fortuity, the “cyber” nature of the loss becomes considerably less important—perhaps even irrelevant. When cyber risk is treated more as risk and less as cyber, coverage questions involving loss or liability can be dealt with more cleanly and arguably less expensively through avoidance of unnecessary or protracted litigation.

This article examines the degree to which cyber losses differ from other insured losses. The cyber-loss insurance coverage jurisprudence reveals a mishmash of principles and coverage terms¹ that are largely focused on the technology of the loss and not on the nature of the loss insured. Unpredictable and unhelpful analogies have ensued, prompting a highly inefficient coverage marketplace and resulting litigation experience. This article also draws parallels with the market experience of a number of now-commonplace insurance coverage products, like CGL policies, that also went through an initial period of uncertainty. Lessons from those prior insurance experiences are instructive as the wild world of cyber insurance stabilizes.

The long-term solution is for insurers to simply fold cyber-loss coverage into traditional coverage products and not differentiate a loss based on its particular or peculiar property characteristics. The focus should be on the risk presented in the context of the policyholder’s ordinary operations rather than the corporeal characteristics of lost or allegedly injured property.

The path to that long-term solution will undoubtedly follow the same pattern as all the insurance industry’s attempts to deal with past “novel risks” at which insurers originally balked. That history starts with adding to what was once mere fire insurance coverage, extends through the bundling of many liability coverages into the CGL policy, and, finally, culminates in the amalgamation of coverage modules governing various aspects of modern business. This amalgamation of coverage continued to now include not only physical injury to property of the policyholder or third parties but also injury once regarded as intangible, as well as injury or losses particular to modern or “high-tech” businesses quite different from the smokestack factories that spawned industrial insurance.

These insurance industry attempts to map out coverage for such risks typically involved an initial period of coverage denial under

1. See, e.g., Robert H. Jerry, II & Michele L. Mekel, *Cybercoverage for Cyber-Risks: An Overview of Insurers’ Responses to the Perils of E-Commerce*, 8 CONN. INS. L.J. 7, 9 (2001) (“[I]nsurers’ responses to [cyber-loss coverage] have been anything but uniform.”).

traditional policy language, as courts attempted to inefficiently analogize to coverage issues in the past and differentiate based on largely arbitrary qualities of new property, activity, or risk. Today we see this in the disparate rulings surrounding coverage for cyber losses.

In the past, these episodes have resulted in new and varying insurance products targeted at this specific “new” risk (as occurred, for example, during the Year 2000, or “Y2K,” perceived “crisis”).² The speed with which the market responds may vary. But history suggests the market will eventually respond and crystallize with acceptance of the “new” risk, recognizing it as a “new normal,” and that coverage for cyber losses can indeed follow along the same lines as coverage for similar risks that do not have the “cyber” quality to them.

This movement may start with the new cyber coverages showing up as drop-down coverage, or endorsements, to attach to traditional insurance product lines. However, we expect that those additions will soon become permanent mainstays in most standard CGL, directors and officers, and homeowners insurance policies. We wish this circuitous route could be avoided but insurance, necessarily being a world anchored in the study of past happenings, is difficult to move without actuarial evidence on which to base innovation. That is why our short- to medium-term solution is an interpretive framework, until such time that modern-day insurance realizes that cyber losses are part of the modern world as much as house fires or burglary.

Ultimately, however, the correct answer—for both policyholders who want protection, and insurers who want profit—is inclusion of cyber-loss coverage in the basic property and liability policies purchased by the bulk of businesses and consumers.

II. THE COVERAGE LANDSCAPE FOR CYBER LOSSES

The current coverage market for cyber losses is a patchwork network of both traditional insurance products as well as new, cyber-loss-specific insurance policies like network security policies or cyber-insurance policies.³ A “cyber loss” refers to a loss or liability arising out of the use of electronic equipment or electronically stored information. Cyber losses include such things as cyber security breaches, data losses,

2. See generally Jeffrey W. Stempel, *A Mixed Bag for Chicken Little: Analyzing Year 2000 Claims and Insurance Coverage*, 48 EMORY L.J. 169 (1999) (detailing the remarkable wind-up that occurred in the insurance world immediately prior to the Year 2000 computer bug that never really materialized in the scope and scale of losses expected).

3. Such as CGL policies and directors and officers liability policies. See, e.g., 2 JEFFREY W. STEMPEL & ERIK S. KNUTSEN, STEMPEL & KNUTSEN ON INSURANCE COVERAGE § 23.04 (4th ed. 2016) (discussing the anatomy of cyber-risk insurance).

infection with computer viruses,⁴ breaches of data privacy,⁵ unauthorized access, release or publication of private electronic information,⁶ mis-transfer of electronic funds,⁷ or losses due to computer mishaps, malfunctions, or misuse.

A cyber loss could result in a first-party claim whereby a policyholder claims under its own insurance policy for the losses it suffered. Such claims typically include the cost of the property lost plus business interruption and remediation costs. A cyber loss could also result in a third-party liability claim whereby the conduct of the policyholder triggers a lawsuit from a third party who alleges that the policyholder's behavior caused a cyber loss for that third party.

There is no doubting the cost of cyber losses to policyholders or third-party victims of a cyber loss. A simple data breach can cost a policyholder millions of dollars to remediate.⁸ Banks and other large institutions that deal in large volumes of customer data or with sensitive financial or health data are especially susceptible to cyber losses stemming not only from negligence but from cyber crime and fraud as

4. See, e.g., *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802–03 (8th Cir. 2010) (applying Minnesota law to a case involving a customer infected by spyware from an online advertising retailer).

5. See, e.g., *Zurich Am. Ins. v. Sony Corp. of Am.*, Index No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141, at *1, *3 (N.Y. Sup. Ct. Feb. 24, 2014) (discussing an insurance coverage dispute for a data breach affecting customers of an online gaming network).

6. See, e.g., *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 U.S. Dist. LEXIS 70594, at *91–92 (N.D. Cal. May 27, 2016) (considering a case of wrongful access at a health insurer that resulted in personal health information of 80 million customers being compromised); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 951 (D. Nev. 2015) (examining a claim in which the personal information of 24 million customers was accessed by computer hackers); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014) (discussing a situation in which personal customer information was stolen from an insurance company's computer system), *rev'd in part*, 663 F. App'x 384 (6th Cir. 2016).

7. See, e.g., *State Bank of Bellingham v. BancInsure, Inc.*, No. 13-CV-0900, 2014 WL 4829184, at *2–3 (D. Minn. Sept. 29, 2014) (describing a case in which a hacker gained access to a bank computer system through spam email and computer virus, and the bank was duped into transferring funds to Poland), *aff'd*, 823 F.3d 456 (8th Cir. 2016).

8. See PONEMON INST., 2017 COST OF DATA BREACH STUDY 1 (2017), <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN> (noting that, in 2017, the average total cost of remediation efforts with respect to data security breaches for financial institutions was \$3.6 million per incident).

well.⁹ Cyber attacks could even feasibly lead to physical injury to property or persons.¹⁰

The insurance market for cyber losses is a patchwork market that is highly—but imperfectly—segmented.¹¹ It is patchwork because there are both traditional insurance products and new cyber-specific insurance products available on the market. The cyber-specific products may exist as add-ons to presently existing coverage lines, in the form of endorsements or drop-down coverage,¹² or they may be independent, stand-alone coverage products that may target only certain cyber losses. The insurance market has been exploding with a variety of cyber-specific products. Such products provide insurance coverage for losses such as security breach expenses, electronic data remediation costs, business interruption, and electronic and payment expenses.¹³

It is an imperfectly segmented market because what a traditional, non-cyber-specific insurance policy excludes from coverage may or may not be covered by an available cyber-specific policy on the market. For example, the Insurance Services Office, Inc.’s (ISO) standard CGL policy endorsement form excludes from coverage “data-related liability,” which includes liability arising out of “loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.”¹⁴

In that same policy, “electronic data” is defined as “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

9. See PONEMON INST. & ACCENTURE, 2017 COST OF CYBER CRIME STUDY: INSIGHT ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE 20 (2017) (noting that the average cost of cyber crime for large financial services companies in 2017 was \$18.28 million).

10. See, e.g., Nicole Perloth & Clifford Kraus, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, N.Y. TIMES (Mar. 15, 2018), <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html> (discussing how a hacking attempt of a petrochemical manufacturer appears to have sought “to sabotage the firm’s operations and trigger an explosion”).

11. See TOM BAKER, INSURANCE LAW AND POLICY 466–67 (2d ed. 2008) (noting that the concept of market segmentation is prevalent in the insurance market, and insurers divide insurance products based on certain grouped underwriting risks such as auto risks for auto policies and commercial risks for commercial policies).

12. See, e.g., *Doctors Direct Ins., Inc. v. Bochenek*, 38 N.E.3d 116, 119 (Ill. App. Ct. 2015) (featuring a cyber claims endorsement on a professional liability policy).

13. 2 STEMPER & KNUITSEN, *supra* note 3, § 23.04 (discussing the anatomy of cyber risk insurance). The 2015 Cyber Risk Solutions form from ISO provides these, and other, first-party coverages. INS. SERVS. OFFICE, INC., ISO CYBER RISK SOLUTIONS FORM z14181 (Mar. 2015).

14. INS. SERVS. OFFICE, INC., COMMERCIAL GENERAL LIABILITY ENDORSEMENT FORM CG 21 07 05 14, at 1 (2013).

devices or any other media which are used with electronically controlled equipment.”¹⁵

Because of these broad definitions of electronic data excluded from coverage, the wide variety of cyber-specific products on the market may only fill some of the gaps left in this exclusion and may well provide additional coverage unique to a CGL’s traditional scope.¹⁶ This has resulted in somewhat unpredictable and uncomfortable insurance coverage gaps for cyber losses.

The cyber-insurance market has only recently developed, and often has developed in direct response to the evolving continuum of cyber losses. It is not a market that, at present, appears to be driven by perfect symmetry with traditional insurance coverage for non-cyber losses. A policyholder’s coverage for cyber losses depends not only on what is covered and excluded by his or her standard insurance products, but also on what is covered and excluded by whatever cyber-specific insurance he or she has purchased.

The landscape for cyber-loss insurance coverage has, therefore, been tricky for policyholders and insurers to navigate. New products, untested policy terms, and issues with how the coverage synchronizes with traditional non-cyber-insurance products have plagued the developing coverage jurisprudence. The result has been striking inconsistencies among the cases and ballooning litigation as the cyber-loss coverage landscape is tested by policyholders expecting coverage for cyber losses.¹⁷

At the same time, inconsistencies and litigation have also been fueled by courts’ peculiar approaches to cyber losses in the context of coverage litigation. In the cyber-loss sphere, courts have, for the most part, been trapped in unhelpful analogies differentiating cyber losses from losses that occur in the physical world. Rather than focusing on the inherent nature of the loss and its place in the panoply of available insurance coverage for cyber risks, courts instead become enraptured by the technological differences between a cyber loss and its parallel in the non-cyber world.

As will be shown below, those differences are often misleading and lead to troubling, inconsistent coverage determinations that damage the ultimate stability of the cyber-insurance market. This problem is compounded by the rapid development of a segmented insurance market

15. *Id.*

16. Such as coverage for identity theft reparations, for example.

17. See Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 253 (2017) (discussing the significant uptick in cyber-insurance litigation cases filed from 2011 to 2015).

for cyber losses that is not consistent with the reasonable coverage expectations of the modern policyholder.¹⁸

III. THE PHYSICAL-DIGITAL CONUNDRUM FOR CYBER LOSSES

Policyholder losses in the cyber world are no different in end result than the traditional physical losses incurred due to negligence. A policyholder facing breach-of-privacy cyber liability—whereby some estimates put the cost of each compromised customer record at about \$140 of liability¹⁹—is surely in a better position than one facing claims for groundwater pollution, adverse reactions to medicine, or injury or damage from a toxic substance. But in extreme cases of such liability exposure, insurers have reacted by excluding significant claims from basic coverage through the asbestos exclusion and the pollution exclusion.²⁰

The question then becomes this: How different is cyber loss than the types of risks—in terms of frequency and magnitude—that are already bundled into the comprehensive property and liability insurance widely sold throughout the industrialized world?

To be sure, because of the multiplying network power of the Internet, the magnitude of the risk may be large. But is it any larger than the magnitude that exists for manufactured products in wide distribution? In many cases, the answer to that question is a resounding “not much.” Manufacturers process millions of credit card or other payment transactions each day. If something goes wrong, third parties can lose money. But these same manufacturers also produce tens of thousands of products that may cause physical injury or even death.

Assessing underwriting issues in this manner leads to a simple conclusion: None of these aspects are, at heart, issues about insurability and coverage. Instead, they are issues about wise-insurer *ex ante* underwriting: Did the premium charged match the scope of the risk insured?

None of these issues involve serious over-arching moral hazard or adverse selection issues that prompt questions about whether the loss was

18. See Amy R. Willis, Note, *Business Insurance: First-Party Commercial Property Insurance and the Physical Damage Requirement in a Computer-Dominated World*, 37 FLA. ST. U. L. REV. 1003, 1022 (2010) (predicting that business insurance products will become “wholly inadequate” to modern business needs as cyber losses become more ubiquitous).

19. See PONEMON INST. & ACCENTURE, *supra* note 9, at 1.

20. See 2 STEMPEL & KNUTSEN, *supra* note 3, §§ 14.01, 14.07, 14.11 (describing the evolution of the CGL form and the 1986 revision to the form that introduced broadly worded exclusions for asbestos-related liability, government-mandated environmental cleanup, and pollution).

fortuitous and, thus, uninsurable. These losses are not certain to occur as a result of the policyholder's behavior.

Thus, cyber losses are theoretically insurable as part of a comprehensive insurance product. The proliferation of cyber-insurance products and the policyholder's challenges in obtaining post-loss coverage under those products can, to date, be explained by the insurance industry riding the uncertainty wave as courts grapple with cyber loss legal issues in policies with non-standard language and coverage frameworks.

Cyber losses currently fit into four general categories of insured loss that are typically covered in their non-cyber forms in traditional property and general liability insurance products: property losses, losses due to crime or fraud, liability for property losses to others, and liability for privacy-related losses to others.

Each type of loss is typically excluded from coverage in its cyber form under traditional products in two possible ways: either as not meeting conditions for coverage as a "direct physical loss" to property that is "tangible,"²¹ or, if covered, by then being an excluded loss caught by an "electronic information" type of exclusion. The secondary market for cyber-specific policies attempts to fill in the gaps, albeit in a piecemeal kind of way.

Cyber-property losses include the loss of sensitive electronic data or damage to computer equipment or software. If a large online retailer loses its customer database of millions of people, such is an incapacitating loss to the retailer. There is an inherent economic value to these commercial data tools in that they are a capital asset to the retailer. But the loss, in kind and even in degree, is not inherently different than if a more traditional, paper-based retailer lost the information for all of its customers when the customer rolodex burned up in an office fire. If the paper goes up in smoke, the non-cyber loss leaves the policyholder in the same place—without valuable customer data.²²

21. The standard all-risks property policy provides coverage for "direct physical loss" to property that is "tangible." *See, e.g.,* Metro Brokers, Inc. v. Transp. Ins. Co., No. 1:12-CV-3010-ODE, 2013 WL 7117840, at *1 (N.D. Ga. Nov. 21, 2013) (providing an example of a standard property coverage clause); *see also* Willis, *supra* note 18 (concluding that the "physical damage" grant of coverage in property insurance should be interpreted in an expansive way to catch cyber losses).

22. *See, e.g.,* Liverpool & London & Globe Ins. Co. v. Kearney, 180 U.S. 132, 135 (1901) (describing a situation in which business records were destroyed in a fire when a fleeing policyholder forgot to place records in an iron safe as required by the policy, and despite the breach of this warranty, coverage was granted); Harris v. Albrecht, 86 P.3d 728, 730 (Utah 2004) (detailing how a fire destroyed an architect's home office and drawings valued at more than \$1.1 million, and finding no coverage for the drawings because the policy at issue contained an exclusion for business operated on the insured property).

The loss of the customer database is a loss of property that will almost certainly result in business interruption losses of some kind until the data is rebuilt. Additional property-related losses could also include the cost to rebuild the database and the loss of the capital asset itself, which has an inherent value. The cyber version of this loss just seems more likely to occur than the office fire because it could happen due to a computer virus, an incorrect keystroke by an employee, or some other software failing. Additionally, that same loss could occur if the servers backing up the customer data get burned up in a fire.

But—inconsistently in our view—traditional property insurance would cover the paper loss as “direct physical loss” to “tangible” property—and the resulting interruption, if business interruption coverage were part of the policy—but likely would not cover the cyber version of the loss, which would be caught under the “electronic information” exclusion.²³

For example, there was no coverage for corrupted computer data claimed under the policyholder’s CGL policy at issue in *America Online, Inc. v. St. Paul Mercury Insurance Co.*²⁴ In that case, the court found that computer data was not “tangible property” and the loss was not caused by the policyholder’s faulty product because the computers were not physically damaged in any fashion. The data was just corrupted and rendered unusable. Yet, to the court, “tangible property” had to have some physical substance that was apparent to the senses.²⁵

Contrast the *America Online* court’s treatment of data with the loss of custom programming at issue in a business interruption claim in *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*²⁶ In *American Guarantee*, a power loss resulted in the policyholder losing customer programming, which prevented the policyholder from conducting business for an eight-hour period. The court held that

23. See, e.g., *RSVT Holdings, LLC v. Main St. Am. Assurance Co.*, 25 N.Y.S.3d 712, 713–14 (N.Y. App. Div. 2016) (describing a data breach at a burger chain that resulted in a lawsuit to replace 1,700 debit cards, and finding the electronic data exclusion in the CGL policy barred coverage for the negligent handling of customer data).

24. *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003).

25. See *id.* at 95; see also *State Auto Prop. & Cas. Ins. Co. v. Midwest Compts. & More*, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (“Alone, computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.”); *Ward Gen. Ins. Servs., Inc. v. Emp’rs Fire Ins. Co.*, 7 Cal. Rptr. 3d 844, 851 (Cal. Ct. App. 2003) (holding that the database was not tangible, even though it may have been stored on physical media).

26. *Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000); see also, e.g., *Se. Mental Health Ctr., Inc. v. Pac. Ins. Co.*, 439 F. Supp. 2d 831, 837 (W.D. Tenn. 2006) (finding that a power loss resulting in pharmacy data corruption was a covered “direct physical loss”).

“‘physical damage’ is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.”²⁷

Similarly, in *Ashland Hospital Corp. v. Affiliated FM Insurance Co.*,²⁸ the court determined that the policyholder-hospital could recover for loss of data reliability because excessive temperatures had resulted in a “direct physical loss” to the data, but at a microscopic level, invisible to the naked eye. The conclusion in this case inches closer to blurring the boundary between the physical/cyber-loss divide. Perhaps, however, the *Ashland* court’s conclusion could be explained because the application of an external physical force—heat—to the computers resulted in the data loss.

This is the type of risk in an all-risks policy that the court would expect to possibly attract coverage (as would a power loss in *Ingram Micro*). It is the type of risk courts are used to dealing with in coverage litigation. The loss of corrupted data in the *America Online* case was not covered because its loss of use was due to a series of “computers-only” electronic events, as opposed to the application of some physical external force to the data and its substrate.

Cyber losses due to crime or fraud are also no different in end result than losses due to crime or fraud in the physical world. A bank may be cyber hacked to illegally send monetary wire transfers to illicit accounts, often with the unwitting “help” of a bank employee who creates a lapse in security by opening a spam email or remaining logged in to her computer. But such losses could also happen by more traditional, non-cyber means. A bank employee could forget his key in the bank vault, allowing some interloper to create a distraction and lift some money.

Similarly, a bank employee could be duped into cashing checks or transferring money to incorrect places due to some in-person direction by a fraudster. Bank bond and financial institution insurance would cover the losses occasioned by the traditional bank fraud methods, but many exclude the cyber-related losses, or offload those losses onto more strictly worded add-on cyber-specific products.

For example, a hacker used a computer virus to break into a real estate broker’s online banking system and transferred funds to various accounts in *Metro Brokers, Inc. v. Transportation Insurance Co.*²⁹ The policy at issue provided coverage for “forgery.” The court concluded that this computer funds transfer did not qualify as a covered loss because the

27. Am. Guarantee & Liab. Ins. Co., 2000 WL 726789, at *2.

28. *Ashland Hosp. Corp. v. Affiliated FM Ins. Co.*, No. 11-16-DLB-EBA, 2013 WL 4400516 (E.D. Ky. Aug. 14, 2013).

29. *Metro Brokers, Inc. v. Transp. Ins. Co.*, 603 F. App’x 833 (11th Cir. 2015).

definition of “forgery” in the policy focused on forgery of a “check, draft, promissory note or bill of exchange” and the “signing of a name”: all qualities inherent in the use of the paper form of negotiable instruments. The policy wording did not note the electronic transfer of funds. The hacker in this case used a virus to gain access to computer IDs and passwords, but nothing was “signed.”

Therefore, although there was coverage for the broker for “forgery” of negotiable instruments, those instruments had to exist in paper form and be forged by traditional paper means. It seems questionable that a modern definition of “forgery” involving monetary instruments would restrict itself to paper-based forms only, or that the insurer selling such a product in the modern financial services world would be expecting to cover only paper-based bank losses.

In the liability insurance realm, liability for property losses as a result of negligence in the cyber world is often excluded from traditional liability insurance policies. So, too, are privacy-related losses. The standard exclusions for losses involving electronic data and computers catch these types of losses (i.e., excluding liability for losses of “software, data or other information that is in electronic form”).³⁰ If a company selling online advertising negligently infects one of its clients with a computer virus and renders the client’s computers unusable, there could be a coverage contest as to whether the loss is or is not covered.

This was the case in *Eyeblaster, Inc. v. Federal Insurance Co.*³¹ In *Eyeblaster*, despite the insurer’s arguments to the contrary, the court concluded that loss of use of a computer is loss of use of tangible property, because access to the electronic data stored within is frustrated. The fact that one requires a computer to access the data completes the notion that the loss is “physical injury to tangible property.”

The computer is a physical piece of equipment that is tangible. If the same company that was denied coverage due to data loss from a power surge, virus, or accidental deletion spilled coffee on its own equipment or another’s computer server, rendering that same computer unusable, either first-party property loss or liability to third parties resulting from the spill would, without question, be covered. This dichotomy conflicts with the risk management purpose of insurance for modern businesses.

Similarly, if a retailer has a privacy breach in its million-person customer database and must pay for identity theft rehabilitation for those

30. For example, the CGL policy in *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010), provided liability coverage for “physical injury to tangible property” but excluded from coverage liability for losses of “software, data or other information that is in electronic form.” See *id.* at 801.

31. *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).

million customers, a traditional liability policy would not cover that loss due to the electronic data exclusion. Yet if that same retailer lost its paper-based customer database because the records fell off the back of a truck and were spirited away, liability for loss would generally be covered by a CGL policy.

Each of the above losses has physical and cyber corollaries. Yet in each case, the end result loss is the same to the policyholder, whether the loss occurs in cyber or physical form. The cyber form of the loss perhaps carries a greater risk of incidence. The cyber losses appear to occur more easily because it takes less human interaction to produce a faster, more widespread harm that cannot be contained as quickly as the same loss in the physical world.

But this is a matter of the magnitude of the loss and the speed of its spread rather than a matter of the form of the lost property or injury inflicted on another. Insurers can protect themselves from undue coverage responsibility through policy limits, retentions or deductibles, and higher premiums. Complete exclusions of coverage normally are found only when the peril is too risky for ordinary sales (e.g., war, nuclear disaster, asbestos, pollution) or where the risk insured against is the province of another commonly available type of insurance or is not a risk common to the pool of policyholders as a whole. For example, standard general liability policies exclude liquor liability because most businesses do not serve alcohol. For bars, restaurants, and liquor stores, liquor liability coverage is typically bought in a separate stand-alone policy as needed.³² General liability policies exclude claims arising out of use of an automobile not because the risk is too great, but because this is traditionally the domain of automobile insurance.

32. However, this need not be the case. Although not as counter-productive as separating cyber risk, excluding liquor liability may have become anachronistic in a world where home gatherings, office parties, and receptions serve alcohol and some modern businesses (e.g., internet shoe retailer Zappos and internet reviewer Yelp) permit employees to drink while working as a perk of the job. See Aman Singh, *Drinking at Work: Office Perk or Employee Right?*, FORBES (Mar. 18, 2011), <https://www.forbes.com/sites/csr/2011/03/18/drinking-at-work-office-perk-or-employee-right/#2b029e0526e3> (noting Bloomberg Businessweek report “that Yelp’s headquarters in San Francisco is equipped with ‘a keg refrigerator’ that ‘supplies its employees with an endless supply of beer’”). One of us (Stempel) has visited Zappos HQ in Nevada, where alcohol is available in the company mess hall and may be consumed at work (but we saw no obvious inebriation of the workers). General liability policies could include dram shop coverage, at least by endorsement, and deal with the risk presented through pricing and policy limits or sub-limits. As discussed throughout this article, we see advantages in bundling coverage to the extent feasible. Where coverage is fragmented among different lines of insurance, there will be gaps in coverage varying according to the skill of individual brokers or agents. Where pricing is disaggregated, policyholders will make more “penny-wise, pound-foolish” decisions to forgo purchase of necessary additional coverage where premiums are perceived as too high.

Data can be accidentally erased with the push of a button or the accidental opening of a spam email. In the physical world, while a fire can do the same type of damage, the risk of that fire wiping out physical records is far lower. Today's employees are on the computer keyboards day in and day out, thus increasing the opportunity for an error. The chance of a fire is simply less, but it is not radically different in kind from many losses involving the use of computers and electronics.

Consequently, for cyber losses, the incidence and scope of harm may be higher than in the physical world, at least until the world gets better at technological safeguards, which it undoubtedly will, over time. The exclusions for the cyber versions of these losses persist in traditional liability and property policies, despite the end result losses leaving policyholders in the same place, and despite the prevalence of computers and electronic data in the modern commercial world.

To put the issue in perspective, think about the continuum of technological difference in storing music for personal use. If a policyholder lost her personal music collection and claimed such loss under a property policy, should it matter that the music was stored on vinyl, in 8-track form, on a compact disc (CD), or in digital form? Is not the loss the same to the policyholder regardless of the form in which the property is stored? Insurance does not require physicality to take effect.

Hazel Glenn Beh rightly reminds that standard insurance policies insure many losses resulting from intangible and invisible processes.³³ Damages from pollution or gas, mold, odors, and asbestos are all losses covered by typical insurance policies. They are no less "physical" than electronic processes and can certainly be pervasive, serious losses. In addition, courts are well versed at solving cases dealing with trigger of coverage issues concerning liability for bodily injury or property damage when that damage has not become visible.³⁴

As long as the loss occurs during the policy period, it does not matter to courts whether the loss occurs at a cellular or molecular level, or even if it is visible or detectable at the time. One only has to think of liability for long-latency injuries from asbestos or pollution or contaminated water where the victim does not discover actual harm until years after exposure. Standard insurance policies still provide coverage for those long-latency, "invisible at the time" wrongs. So, when losses occur in the digital world at the level of "ones" and "zeros," carving out coverage based on the "physicality" of the loss at issue seems somewhat

33. See Hazel Glenn Beh, *Physical Losses in Cyberspace*, 8 CONN. INS. L.J. 55, 66 (2001).

34. See 2 STEMPER & KNUTSEN, *supra* note 3, § 14.09[B].

suspect. Those “ones” and “zeros” still exist—they just exist in a different format.

This cyber-versus-physical difference, to us, is an underwriting concern and not a coverage concern. The same type of damage is covered under traditional insurance product lines if the loss occurs in a non-cyber fashion. It is difficult to understand that, in today’s commercial environment where everything is stored electronically and most business is conducted in an entirely electronic fashion, such losses are excluded from the standard, basic, mainstream, and run-of-the-mill insurance products that form the backbone of ordinary risk management and are owned by nearly every business and homeowner (at least in the United States and Canada).

To flip the argument: What good are modern CGL, property, directors and officers liability, and homeowners liability and property policies without coverage for cyber harms? Coverage may not be “illusory” in the most extreme sense. A policy barring cyber-related coverage still provides protection from physical loss. But in the modern world, many consider the Internet and computer access as essential services—a utility as ubiquitous as telephone and water service. For many people, a computer freeze or data loss is dramatically more troublesome than a broken window or a modestly leaking roof.

Nonetheless, the core, standardized policies (homeowners, automobile, and general liability) do not provide coverage for many cyber-related losses. The insurance industry remains in the grip of outdated and perhaps ill-conceived concepts of insurability that unnecessarily hinge on physicality.

To be sure, when computer technology first arrived on the scene, it would undoubtedly have challenged insurance underwriting to predict the scope of losses at play. But at this juncture it seems more than a little irritating that mainstream insurance policies continue to exclude from coverage these now-commonplace losses.

There appears to be no legitimate defensible risk-related argument for failing to include cyber losses within the scope of ordinary risk. Although one cannot discount honest industry apprehension about insuring such risk without separate underwriting focus,³⁵ one need not be

35. See generally Sean M. Fitzpatrick, *Fear Is the Key: A Behavioral Guide to Underwriting Cycles*, 10 CONN. INS. L.J. 255 (2004) (arguing that insurers, despite being in the business of risk shifting and spreading, exhibit risk averse tendencies based on a combination of valid concerns and cognitive errors such as overvaluing a risk that has been highlighted due to recent events). Cognitive psychologists have, for example, identified an “availability heuristic,” in which persons are unduly affected by events reported in the media or recent experiences even when those events pose less risk than more commonplace events that make the newspaper. See Timur Kuran & Cass R. Sunstein, *Controlling Availability Cascades*, in BEHAVIORAL LAW AND ECONOMICS 374,

a cynic to ascribe the situation to insurers taking advantage of market cohesion and a real upsurge in policy sales due to forced market segmentation between insurance products covering cyber and non-cyber losses.

There is little incentive for the industry to rewrite policies to cover these losses unless the market so demands, or unless courts, in their regulatory function, begin to peer through the veneer and realize that certain narrow interpretations of cyber-loss coverage actually nullify the very coverage purchased by the policyholder.

IV. PUBLICATION AND ACCESS HURDLES TO COVERAGE FOR THE RELEASE OF PRIVATE DIGITAL DATA

The same pattern of difficulties in determining coverage with any consistency is exhibited in cases about whether or not electronic privacy breaches are covered under CGL policies. Those cases attempt to fit the coverage language into a landscape where the privacy breach is not through paper-based physical publication but is instead through online means. The fallacies with analogizing to privacy breaches in the physical world lead courts to produce some unexpected and questionable coverage results.

For example, in *Zurich American Insurance Co. v. Sony Corp. of America*,³⁶ the CGL policy at issue did not cover Sony's liability when hackers caused a massive data breach from Sony's PlayStation videogame customer database, releasing millions of gamers' personal identifications and financial information online. Because the hackers were third parties and not Sony, the court determined that the policy did not cover Sony's liability for "oral or written publication in any manner of the material that violates a person's right of privacy." The court determined that the phrase "in any manner" modified the word "publication" and did not relate to how the material was published (i.e., by someone other than Sony, like a hacker). Thus, if Sony itself had accidentally released the data, its liability would have been covered. But because the hackers released the data but used Sony's computers to do it, that was somehow an uncovered event.

This same strict approach to privacy-related electronic "publication" was also followed in *Recall Total Information Management Inc. v.*

381 (Cass R. Sunstein ed., 2000). For example, many people are afraid to swim in the ocean for fear of shark attack, which is extremely rare, but those same folks regularly drive an automobile, which presents a far greater risk of serious injury. See Cass Sunstein, *Introduction to BEHAVIORAL LAW AND ECONOMICS*, *supra*, at 1, 9.

36. *Zurich Am. Ins. Co. v. Sony Corp. Am.*, Index No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 24, 2014).

Federal Insurance Co.,³⁷ where a storage company lost computer tapes that fell off its truck during transport. The owner of the tapes sued the storage company for reimbursement of identity theft services it had to provide to its customers who had their personal data on the tapes. The court found that the loss of the tapes was not a “personal injury” under the storage company’s CGL policy, and thus no coverage attached. “Personal injury” was defined as “an ‘injury . . . caused by an offense of . . . electronic, oral, written or other publication of material that . . . violates a person’s right of privacy.’”

Because the tapes fell off a truck and were retrieved by someone else but not “published,” according to the court, there was no corresponding privacy violation. The potential for wrongful access to the information was not something covered by the policy. The court’s treatment of “publication” required the publication to occur in the traditional sense, at a particular moment in time, rather than through the loss of control of private electronic information such that its publication might occur at some unknown moment in the future (and very easily, because the information exists in electronic form).

Other courts have come to contrasting interpretations as to how electronic information is “published” and whether privacy breaches are covered under insurance policies. When the contents of customers’ online music libraries were released on the Internet by a third-party hacker, the court in *Oscines v. Mt. Hood Insurance Co.*³⁸ held that the CGL policy in question covered the music service’s liability, even though the coverage language was identical to that in the *Sony* case: “publication in any manner.” The court held that “in any manner” did include release by third-party hackers. In *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, L.L.C.*,³⁹ liability coverage for “publication” of private health data that was accidentally available on the public Internet did not hinge on proof of someone accessing that data, as it did in *Recall Total*. The court determined instead that “publication” meant placing the data so that the public can access it—the definition does not require actual access.⁴⁰

These decisions about “publication” of private electronic data run into consistency issues when the concept of cyber “publication” is

37. *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 115 A.3d 458 (Conn. 2015).

38. *Oscines v. Mt. Hood Ins. Co.*, No. 1401-426 (Or. Cir. Ct. July 2, 2015).

39. *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, 644 F. App’x. 245 (4th Cir. 2016).

40. *Id.*; see also Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today’s Litigation, and Tomorrow’s Challenges*, 33 QUINNIPIAC L. REV. 369, 389 (2015) (preferring the court’s reasoning in *Portal* instead of *Recall Total*).

differentiated from traditional publication using printed media. That should not be the case. In today's world, where most media is consumed online and not in hard-copy print format, analogies to the non-digital publication process prompt courts to strike conclusions that are illogical and difficult to port from one context to the next. Instead, courts should focus on the loss claimed, not on the process of the loss. The loss is the cost to repair a data privacy breach—costs that range from credit reporting remediation to identity protection and rebuilding.

Whether the data was accessed by anyone at the time of the claim is not the point—the cost to repair the potential for harm is already borne by the policyholder out of necessity after discovering the breach. Focusing instead on issues of access to the information or how the data leaked and got “published” splits hairs that are not relevant to the loss. Whether the data fell off the back of a truck, was released by a hacker, or was pasted to the web accidentally by an employee asleep at the keyboard, the loss can be traced to some negligent conduct on the part of the policyholder. No policyholder would expect coverage for such a cyber loss to turn on a close reading of terms that would cover the loss if it resulted from a print-based publication.

V. THE MARKET SEGMENTATION NIGHTMARE IN A BRAVE NEW COVERAGE WORLD

The resulting market segmentation between coverage for cyber-related losses in traditional insurance policies and coverage in the myriad of cyber-related insurance products has been nightmarish for policyholders and insurers alike. Naturally, litigation has ensued to test the boundaries of this new insurance language contained in cyber-specific insurance products. The litigation has stemmed largely as a result of four trends in recent cyber-insurance litigation: narrow definitions of covered losses, difficulty with shoehorning claims into pre-determined categories of losses, questions about coverage scope, and challenges to untested moral hazard mitigation efforts baked into the policies themselves.

The resulting gaps in coverage to date have been troubling, as the cyber-insurance world is not lining up with the coverage experience policyholders would reasonably expect had their losses been claimed as physical, non-cyber losses under more traditional insurance policies. This market segmentation nightmare has therefore created somewhat of a wild west of coverage experience in this burgeoning market. That has cost insurers and policyholders alike, as shaky coverage expectations drive up the incidence, and thus the cost, of litigation.

Policies providing coverage for a data breach or data loss have very narrow definitions of what type of loss is covered. Problems of insurance causation can result as insurers and policyholders attempt to bring claims out of, or into, coverage. For example, in *State Bank of Bellingham v. BancInsure, Inc.*,⁴¹ the insurer argued that the bank's financial institution bond providing coverage for "computer systems fraud" would not cover the bank's losses when a computer virus, carried out by spam email, accidentally infected the bank's systems so that a third party could gain access to the bank's wire transfer system. The insurer asserted that the loss did not result from "computer systems fraud" but instead resulted from employee violations of workplace policies regarding computer use, such as failing to control computer password use, enact anti-virus software, or follow policies about spam email.

The court determined that Minnesota's concurrent causation doctrine ensured coverage for this loss because the proximate cause of the loss was the fraudulent virus, not actions by any employee. The result in this case makes sense if one considers the whole purpose of the "computer systems fraud" coverage in the financial institution bond: to protect against fraudulent bank losses. An employee slipping up on following bank policies for payments, while negligent behavior, seems to be precisely the kind of conduct that leads to such financial fraud in the first place. Otherwise, coverage would be negated for the very risk the bank attempted to insure against.

However, the opposite result was reached in *Apache Corp. v. Great American Insurance Co.*,⁴² where a bank employee transferred \$2.4 million to a fraudster who sent an email request to the bank, but used a similar, though not identical, email domain name to a trusted client. The Fifth Circuit concluded that the bank's loss did not result "directly from the use of any computer to fraudulently cause a transfer," but instead resulted from the bank's failure to adequately investigate the identity of the fraudster.⁴³ Causation, in this case, was used as an argument against coverage.

41. *State Bank of Bellingham v. BancInsure, Inc.*, No. 13-CV-0900, 2014 WL 4829184 (D. Minn. Sept. 29, 2014), *aff'd*, 823 F.3d 456 (8th Cir. 2016).

42. *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252, 259 (5th Cir. 2016).

43. *See id.* at 258–59; *see also* *Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627, 628–30 (9th Cir. 2017); *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-12108, 2017 WL 3263356, at *1–4 (E.D. Mich. Aug. 1, 2017); *InComm Holdings Inc. v. Great Am. Ins. Co.*, No. 1:15-CV-2671-WSD, 2017 WL 1021749, at *8–9 (N.D. Ga. Mar. 16, 2017); *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, No. C-14-1368RSL, 2016 WL 3655265, at *1–4 (W.D. Wash. July 8, 2016). In *Taylor & Lieberman*, the court found no coverage under the crime policy at issue when an accounting firm transferred funds due to fraudulent email. *Taylor & Lieberman*, 681 F. App'x at 628. Further, the court found that "forgery" coverage was inapplicable because there was no forgery from the email instruction. *Id.* at 629. Also, the "computer fraud"

This result begs the question: What could this policy cover if not this type of fraud? How “direct” must the computer use be? The result is particularly puzzling in that the denial of coverage is based on a narrow reading of the clause that purports to grant coverage for computer fraud losses.⁴⁴

In addition, policyholders who are liable for the loss or erroneous publication or corruption of client data struggle to shoehorn their claims into ones of privacy, wrongful act, publication, or errors and omissions coverage. Seemingly opposite results were borne out in two cases involving errors and omissions cyber insurance.

In *Eyeblaster Inc. v. Federal Insurance Co.*, the policyholder, an online media company, allegedly infected one of its clients with spyware from one of its online ads.⁴⁵ The client was unable to use its computer and sued the policyholder. The policyholder’s errors and omissions cyber policy (called a “Network Technology Errors or Omissions” policy) was

coverage was found inapplicable because the sending email was not unauthorized “entry into” computer systems, and the fraudulent emails instructing funds to be wired were not “introduction of instructions” that “propagate themselves” through computer systems. *Id.* Lastly, the funds transfer coverage also did not apply because, although the firm did not know the emailed instructions were fraudulent, it was aware funds were being wired. *Id.* at 629–30. This case begs the question: What does the crime policy actually cover? In *American Tooling*, fraudulent emails resulted in wire transfers. *Am. Tooling*, 2017 WL 3263356, at *1. However, because the policyholder verified the production information and authorized payments, the court found that the policyholder did not suffer a “direct” loss “directly caused” by the use of a computer, as these events intervened in that computer use, ousting coverage. *Id.* at *2–3. In *InComm Holdings*, the court found that “computer fraud” coverage requiring “use of any computer to fraudulently cause a transfer” was not triggered when a debit card processing company’s telephonic system was exploited through a coding error and the company lost \$10.3 million in unauthorized telephonic redemptions. *InComm Holdings*, 2017 WL 1021749, at *8. The court concluded that the loss did not result directly from the “use of any computer” to access the telephonic system, even though computers were used in the telephonic system’s operation. *Id.* at *8–9. In *Aqua Star*, a seafood business’s customer hacked and sent fraudulent emails for wire transfers. *Aqua Star*, 2016 WL 3655265, at *1. The crime policy at issue provided no coverage because of an exclusion for “loss resulting directly or indirectly from the input of Electronic Data.” *See id.* at *2, *4. The policyholder’s employee had updated a spreadsheet to include payment information sent by the hacker and the court concluded that this update was a necessary step before initiating the transfer of funds and, thus, an indirect cause of the loss. *See id.* at *4.

44. *See Apache Corp.*, 662 F. App’x at 259. *Contra* Principle Sols. Grp., LLC v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *1–2, *5 (N.D. Ga. Aug. 30, 2016) (describing how the commercial crime policy at issue provided coverage for “computer and funds transfer fraud” when bank transferred \$1.7 million dollars to fraudster’s account as a result of fraudulent email, and finding that the “computer and funds transfer fraud” clause was ambiguous so there was coverage even though intervening events occurred between the fraud and the loss); *Medidata Sols., Inc. v. Fed. Ins. Co.*, 268 F. Supp. 3d 471, 480, 481 (S.D.N.Y. 2017) (finding coverage for computer fraud when fraudulent email resulted in wire transfers because emails contained code that masked hacker’s identity to fool policyholder into approving wire transfer).

45. *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 799–800 (8th Cir. 2010).

triggered because the media company's acts qualified as a covered "wrongful act" that resulted in some product failure. While the insurer argued that the harm was not resulting from a "wrongful act" because the policyholder intentionally placed its software on the victim client's computer, the court rightly concluded that, while the act may have been intentional, the consequences of the act were unintentional and thus "wrongful" under the terms of the policy.

Contrast that result with the result in *Travelers Property Casualty Co. of America v. Federal Recovery Services, Inc.*⁴⁶ There, the insurer was not required to defend a claim against its policyholder, an electronics records processor who claimed under its CyberFirst policy (which featured a technology errors and omissions form), because the policyholder was being sued by a client for withholding data access until the policyholder was paid for its services. The client sued the policyholder for conversion, breach of contract, and tortious interference, but not for negligence. Because none of the allegations involved errors or omissions, the court concluded there was no duty to defend the policyholder.

It seems an odd result that a claim for withholding electronic financial data is not covered under an errors and omissions policy and that the plaintiff's pleading would control that analysis without further consideration of the nature of the allegations pled. This case was dealt with at the pleadings stage, however, and there may well have been some negligence on the part of the policyholder in determining how and why to withhold electronic data. The policyholder was actually in the business of storing and processing electronic data for customers. When sued for issues surrounding that kind of work, the policyholder likely would not have expected coverage to be denied.

This is a different sort of analysis for determining conduct triggering errors and omissions coverage than that of the *Eyeblaster* case. In *Eyeblaster*, although the policyholder-media company's actions were intentional in putting the infected media on the customer's computer, the harm was not expected and was borne of negligence. One could make a similar argument in the *Federal Recovery* case that while the withholding of data services in the expectation of payment may have been an intentional decision, the resulting harm to the client was entirely unintentional (and, although perhaps dirty pool vis-à-vis commercial relations, was probably borne of negligence in managing payment risk).

Some policyholders experience gaps in coverage because the current cyber-insurance market has yet to have the experience or

46. *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.*, 103 F. Supp. 3d 1297, 1302 (D. Utah 2015).

foresight to predict how reasonable losses may be incurred as a result of cyber-related behavior.⁴⁷ An entity that must compensate a third-party financial institution for losses from data breach may be surprised to learn that coverage under many cyber policies only attaches if the policyholder-entity, and not the third-party financial institution, is the target of a wrongful act. This can be true even though the financial institution is the processor of all transactions for the policyholder and can pass along the costs of such wrongful acts to the policyholder.

For example, in *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*,⁴⁸ when a hacker posted thousands of restaurant customer credit card numbers to the Internet, the restaurant was charged a substantial fee from a major bank that processed the credit card transactions because the credit card company's own fraud recovery costs were charged to the bank (for fraudulent transactions from the published credit cards). The restaurant's insurer refused to cover the fee the bank levied on the restaurant because the policy provided coverage for a "privacy injury" and the insured was the restaurant, not the credit card company or the bank processing the transactions. Even though the restaurant had a contractual arrangement with the bank about the responsibility for fees relating to data breaches, the court determined that the fees the restaurant had to pay the bank were not because of a "privacy injury" to the policyholder.

This result exposes a failure as to how cyber-loss coverage is presently designed to respond to the entire scope of a loss for a modern "privacy injury." The loss to the restaurant is substantial and borne precisely because of the data privacy breach that spawned the claim to the insurer. However, because the loss was realized from the restaurant's contractual relationship with its suppliers, the loss was excluded from coverage. On the one hand, one can argue that the dealings of policyholders with various entities are not the subject of insurance. Otherwise, how could an insurer control risk exposure if it had to cover losses that were controlled by contractual dealings with third parties?

On the other hand, this is precisely a predictable—and insurable, at least in concept—expense from a data breach. It is foreseeable that one loss from the leak of customer financial information would be the remediation cost a third-party financial institution would have to undertake when making good for wrongful credit card payments. To have that cost passed back to the restaurant seems sensible and consistent

47. See Podolak, *supra* note 40, at 372 (raising the issue that current cyber risk insurance policies may not be accurately predicting the full scope of data breach expenses suffered by policyholders).

48. *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).

with insurance concepts of subrogation. Yet to have that loss excluded from coverage for the “privacy injury” seems a stretch. Many commercial establishments would be caught unaware, to say the least.

Finally, a surprising number of cyber-insurance policies incorporate various pre-loss cyber-security requirements to which a policyholder must adhere in order to obtain coverage post-loss. Some include standards to which data must be kept. Others require security processes and policies to meet a specified standard. Still others demand that policyholders have undergone pre-loss training or security audits before coverage will attach under the policy.

In *Columbia Casualty Co. v. Cottage Health Systems*,⁴⁹ for example, a health organization that experienced a server breach that compromised the confidentiality of medical records for 32,500 patients turned to its “NetProtect360” cyber-insurance policy for coverage when faced with a class action in response to the breach. The insurer sought recoupment of defense costs because it alleged the organization misrepresented that it took security steps required by the policy’s “Failure to Follow Minimum Required Practices” exclusion. Specifically, the insurer alleged the health organization did not properly maintain its servers to prevent access by outside computers nor did it properly monitor for unauthorized access data.

The aim of these sorts of pre-loss electronic security requirements is to mitigate moral hazard by ensuring the policyholder adheres to some basic data security standards. Of course, who sets the standards and what the standards include are the live issues. Uncertainty abounds as various policies have differing requirements for “pre-coverage” standards to be met. It is the insurer setting the data standards, which may or may not be reasonable in today’s commercial market. How is a policyholder to know whether it can, or even should, meet insurer-set data security standards? How is a policyholder to know those insurer-set standards are up-to-date, relevant, and appropriate?

In addition, this type of extra-contractual behavior requirement can act to neutralize coverage based on some third party’s behavioral standards. This is a marked change from the non-cyber liability insurance context, where policyholder negligence (i.e., the tort standard) is used to trigger liability coverage. Instead, in the cyber-insurance context, a perhaps time-stamped and ephemeral insurer-chosen standard of pre-loss behavior acts as an ever-moving gatekeeper to coverage. Policyholders are left to navigate this uncertain coverage landscape.

49. *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432, 2015 WL 4497730 (C.D. Cal. July 17, 2015).

What is even stranger about the *Cottage Health Systems* example is that the pre-loss computer security requirements demanded by the insurer are acting as post-claim underwriting opportunities for the insurer. The insurer sells the policy, then trusts that policyholder representations about various computer security protocols are true. After the loss, if the policyholder has not met the insurer-specified behavioral standards, that insurer can back out of coverage. This is akin to an attempt by the insurer to eliminate substantially all risks and is not really an issue aimed at regulating policyholder moral hazard with respect to computer security.

If a policyholder had perfect compliance with computer security, the risk of loss should be zero. Put another way, as long as the data security loss is fortuitous, and the policyholder acted reasonably in general toward network and data security, the loss should be covered. Resting coverage on the specific instance of policyholder behavior through which the very claim arises seems somewhat suspect.

Much of the haphazard nature of coverage litigation to date with cyber-insurance policies can be expected with the variety of products, policy wording, and level of underwriting experience of insurers with cyber claims thus far. For this reason, as time marches on, one can expect that the market will become more streamlined in terms of policy forms and litigation experiences. However, in the meantime, beyond structural issues of market variance, the market segmentation problem is vastly augmented because of the trappings of language and thought anchored in the physical, non-cyber world.

VI. THE REACTIONARY APPROACH TO “CYBER” ANYTHING

Coverage gaps and increased litigation uncertainty in the cyber-insurance world are mainly stemming from an unhelpful—and probably inaccurate—approach toward the nature of cyber losses. As mentioned above, cyber losses may differ in degree, but not in kind, from losses in the physical world. But, for the most part, cyber losses do not differ at all from physical-world losses. The nature of property and liability have necessarily changed with the impact of the digital world. It is about time the insurance world caught up to it. The dangers to policyholders and insurers alike in this new cyber-insurance world stem from two trends: unhelpful analogy to the physical world and insurance market overreaction.

The coverage scope of non-cyber-specific policies often excludes cyber-related losses. As we explained above, for historical reasons, the scope, kind, and degree of loss may not have been knowable at the time the exclusions appeared on the market. Surely, however, by now, computers are not new to the world. Yet the exclusions remain. It is as if

insurers are pretending that it is still 1984 and the world is wondering what will happen next with computers. At the time of the introduction of computers to commerce, and life in general, insurers could be forgiven for being understandably wary and excluding such losses from coverage until the world stabilized. But nowadays?

The result has been that insurance policies, including both cyber and non-cyber, are running on analogies to policy language built for the physical world. These analogies simply do not work anymore. For example, a property policy typically covers “direct physical loss or damage.” Cases abound about whether or not a cyber loss is a “physical loss.” It is not physical in the sense that the bits of data cannot be touched. Yet the data exists, as a series of ones and zeros at least, somewhere. The loss to that data is often not occasioned by the traditional causes of loss: physical force to an object. The loss is often triggered through some user step, like a keystroke, that is not in and of itself harmful. Or stranger still, the loss is often occasioned by a computer hacker or virus.

Courts struggle with how to analogize the apparent lack of “physicality” of electronic data to how lightning strikes a house or fire burns up papers. That struggle typically devolves into a discussion about the very nature of the specific technology at issue and how it operates differently as compared to how a similar loss might operate in the physical world. The analysis just about never focuses on the nature of the loss as a loss in and of itself.

While law is itself a self-referential exercise that relies on past case precedent and *stare decisis* from which the bedrock of the legal system comes, in the cyber-insurance sphere, the system is relying on past analogies that just do not work. The focus of the analysis should be on the core risk management principles embedded within the insurance product—fortuity and the bargained-for protection from fortuitous losses—not on how the loss actually happened and its “cyber-esque” quality that makes it “different” from physical-world losses.

The pattern of courts overblowing new developments with fanciful and apocalyptic analogies is not a new one—and certainly is not new in insurance law. One only has to look to the Year 2000 bug hype in the late 1990s to see how an explosion of Y2K insurance coverage products and concerns came to naught as the Y2K issue itself came and went with nary a whimper. This “chicken little” response of the legal sky about to fall was put best by one of the authors as this: “A new development is

treated as if it is a new type of law rather than an old type of law in a new context.”⁵⁰

That statement works equally well for both the courts’ approach to cyber-versus-physical analogies in coverage cases and the insurance industry’s market response to cyber losses. In an attempt to maintain its current market-segmented stance but, at the same time, capitalize on the potential profit source of coverage for cyber-related losses, insurers have developed new products in new policy forms with new coverages that did not exist before (at least with untested language).

The pattern above of court interpretation of novel coverage terms is also not new or unique to the cyber-insurance world. The insurance world has had past experience with new forms of coverage or the introduction of major exclusions. The interpretive pattern in the courts has been similar. The interpretation typically starts with a broad, far-reaching interpretation, which is very quickly narrowed down to something more measured in result. Then, the interpretive results get a sort of ratcheting back up in a more nuanced fashion to something of an interpretive equilibrium (with concomitant redrafting of policy language to something more appropriate—a reasonable response from insurers). The classic example of this pattern is the court experience with the standard pollution exclusion in CGL policies or the interpretation of business interruption coverage in CGL policies.⁵¹

Outside of insurance, we saw a similar phenomenon in civil procedure with the advent of the Internet. Courts then faced questions regarding whether emails or websites (passive or active) supported the exercise of personal jurisdiction. After a decade or so of fits and starts, a body of law emerged that sensibly applied traditional “minimum contacts” personal jurisdiction analysis in this new context without the need for special rules for cyber contacts with a forum.⁵² Issues regarding electronic discovery proved more difficult and prompted special amendments to the Rules of Civil Procedure, as well as long analyses by groups such as the Sedona Conference.⁵³ But, in our view, some of this trip may not have been necessary. The better-reasoned decisions

50. Stempel, *supra* note 2, at 174 (predicting, in 1999, that the insurance experience post-Y2K would not be “Armageddon”).

51. See, e.g., Beh, *supra* note 33, at 77 (noting the necessary transition period that traditional insurance product lines will face due to attempts to sort out coverage issues for cyber losses); Jerry & Mekel, *supra* note 1, at 26 (tracing the evolutionary path of commercial liability insurance and particularly the “erosion” of comprehensive business coverage as e-commerce exclusions emerge).

52. See JEFFREY W. STEMPEL ET AL., *LEARNING CIVIL PROCEDURE* 118–19 (2d ed. 2015).

53. See JANET WALKER ET AL., *THE CIVIL LITIGATION PROCESS: CASES AND MATERIALS* 456–59 (8th ed. 2016).

regarding electronic discovery simply apply time-honored concepts of relevance, privilege, burdensomeness, and spoliation to records that are electronic rather than paper.

The genesis of the modern CGL insurance policy and even the homeowners insurance policy also display a similar pattern of product development.⁵⁴ Those policies each went from initial offerings of broad, all-risks coverage at market introduction to (very quickly) a coverage offering riddled with exclusions to a backing-off and recent augmentation of certain forms of coverage (like identity theft coverage now becoming more standard in homeowners policies, for example).

We expect the same interpretive and market patterns to occur with cyber-loss coverage, with one major exception. We predict and expect that cyber coverage will, by necessity, become folded into standard insurance products' coverage offerings. The digital age is well past due. Requiring patchwork coverage solutions to now standard losses will quickly become untenable in the insurance market.

Indeed, the removal of some cyber losses from standard coverage may do such violence to policyholders' reasonable expectations of coverage as to nullify the very purpose for which the insurance was purchased, and, thus, invalidate an off-coverage response. The gaps in coverage created by artificial market segmentation will expose market opportunities and market failures. Insurers are nothing if not opportunists, and for good reason. Being able to charge a single (perhaps enhanced) premium for a one-stop shopping product that covers traditional and cyber losses in one policy, without distinction, is the natural outgrowth of the market.

A cyber-neutral product will be the next stage of the insurance product genealogy because, otherwise, not only will the market capture rate increase for insurers, but also the cost of uncertainty of many patchwork policies operating with as-yet-untested language will be problematic at best. Litigation will result. The cost of analogies to the physical world and the interpretive uncertainty of cyber-specific language will funnel insurers, we expect, to create an all-in policy—and in short order.

We expect this market response from insurers because we have seen this type of policy conglomeration before. Coverage that was once only available as an add-on through endorsement or drop-down coverage thus gradually creeps into the main coverage grants of a standard general policy over time. Policyholder expectations of coverage, at some point,

54. See KENNETH S. ABRAHAM, *THE LIABILITY CENTURY: INSURANCE AND TORT LAW FROM THE PROGRESSIVE ERA TO 9/11 (2008)* (tracing the history of the development of liability insurance and its pervasive growth and effect on compensation for losses).

become so entrenched that arguments about coverage nullification for exclusion of standard losses become costly arguments for insurers to meet.

As standard coverage terms in a policy morph and begin to delineate more prevalent covered losses, it is forgotten that the coverage piece was actually once only available as a standalone product or as a tacked-on endorsement. The identity theft coverage that is currently standard in most homeowners' property policies is an example of coverage that was once, very recently, only available sparingly, and at an extra expense for an additional rider to the policy. Now, it is incorporated into most policies as baseline coverage. Business interruption coverage was once a rare, add-on coverage to the CGL policy. Now, it is commonplace in most CGL policies.

One can even trace this pattern back to the dawn of fire insurance that protects the private dwelling. Today's homeowners' property policies cover multiple perils beyond simply fire and also cover far more than the mere dwelling to include outbuildings and other structures detached from the dwelling, as well as personal contents of the home. The cyber-loss market will soon, we expect, start to provide cyber-related coverages in traditional lines of insurance as drop-down, or add-on, coverage (likely for modest premium increases to account for the additional risk underwritten).⁵⁵

Coverage for cyber losses will necessarily follow this same route simply because the commercial insurance market will demand it. Today's current market segmentation of cyber products is, in all likelihood, a false and time-limited segmentation. The losses are not discrete between lines as they are between auto and non-auto policies, or between commercial and homeowner liabilities. The distinction between cyber and non-cyber losses is blurry at best, non-existent at worst. So, the eventual collapsing of the cyber lines into appropriate traditional insurance products fits with market expectations. Once one carrier offers a cyber-neutral policy, other carriers will have no choice but to follow suit. For who can run a business in today's world without using computers and digital data and thus without embracing some degree of risk from that use?

55. See JOHN BUCHANAN & DUSTIN CHO, ABA LITIG. SECTION, INS. COVERAGE LITIG. COMM., WHEN THINGS GET HACKED: COVERAGE FOR CYBER-PHYSICAL RISKS (2016), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2016_insurance_coverage_litigation_committee/written_materials/2_cyber_physical_harms_paper_final.authcheckdam.pdf (predicting that the cyber-market will blossom in this fashion, with drop-down coverage on product lines like directors and officers liability insurance).

VII. THE INTERIM SOLUTION: A TECHNO-NEUTRAL APPROACH TO POLICY INTERPRETATION

In the interim, before the insurance market responds with cyber-neutral policies, the plethora of cyber-specific insurance coverages will continue to clash with the non-cyber coverages. Gaps in coverage will mutate. The interpretive landscape will be in flux. Litigation will remain a constant. To weather this transition period, we suggest that courts adopt a technologically neutral stance to the interpretation of insurance policy language when faced with a coverage question involving a cyber loss. By focusing on the nature of the loss itself, rather than its “cyber” quality, and by grounding the interpretive analysis in basic bedrock insurance principles of risk management and fortuity, courts will avoid the trap of falling into unhelpful analogies to losses in the physical world or creating unrealistic expectations for policyholders and insurers attempting to determine coverage. We recognize that while it may well be that a few savvy insurers are already developing cyber coverage products that respond to a wider, more comprehensive array of cyber-related risks by using more broadly worded coverage grants than have typically featured to date in the case law, a techno-neutral jurisprudence will support those insurer efforts by providing an effective nudge to the less savvy insurers who are holding back the pack.

We suggest an interpretive solution because the tools of insurance policy interpretation can quickly respond to a number of the issues with emerging cyber coverage while the market sorts out how it will begin the process of more holistically bundling cyber losses into standard insurance products. For example, one tenet of interpretation holds that an exclusion from coverage should not take away the very coverage purportedly provided by the policy in the first place. A policy that provides coverage for bank fraud cannot exclude coverage for bank fraud as it reasonably most likely occurs in modern banks.

Another axiom of contract construction requires courts to interpret coverage clauses broadly and exclusion clauses narrowly.⁵⁶ In the cases discussed in prior sections, many courts turned this rule of construction on its head and erroneously took very narrow approaches to coverage provisions found in cyber policies, reaching results we (and most observers outside insurance companies) regard as incorrect. Applying these standard concepts of construction in a fashion neutral to the technology behind the loss will help courts reach consistent and correct determinations.

56. 1 STEMPEL & KNUITSEN, *supra* note 3, § 4.04.

Techno-neutrality⁵⁷ means treating the language of the policy without regard to whether the loss is cyber-based or confined to the tangible physical world. Techno-neutrality also means treating the loss itself as the inherent resulting loss, and not according to its causality (cyber or non-cyber). If it is true that cyber losses are just as insurable as their parallel physical losses and still cause the same economic harm to a policyholder, then the coverage question must necessarily shift to: “Why is the physical loss covered but the cyber loss not?” Examining that question leads a court to look at the inherent nature of the loss to the policyholder and the type of coverage granted by the insurer.

In other words, the court should look at a category of loss independent from its physical or electronic properties. For example, if a coverage grant includes coverage for losses relating to a customer database if that database exists in a physical form but not if it exists as electronic data, a court should approach the coverage question from a techno-neutral stance and ask: Did the insurer here mean to cover losses relating to customer databases at all? If so, did it only mean to cover such losses if they occurred in the physical form? If the answer is “yes,” and absurd results follow because coverage becomes largely illusory, this suggests a problem with the policy.

A court should then ask what reasonable policyholders and insurers would expect from the coverage. For example, a policyholder that had purchased crime insurance would, presumably, be horrified to find out that a million-dollar swindle was not covered merely because it was perpetrated via email rather than over the phone. Similarly, a policyholder that purchased cyber-crime insurance can hardly expect to lose coverage on the ground that the swindle could have been accomplished over the phone as well as via email.

Exclusions are often broadly written to apply to any loss “arising out of” cyber activity or whatever other peril the insurer seeks to remove from coverage. Insurers are free to write exclusions broadly even if this is inconsistent with the nature of the coverage sold to the policyholder. But courts are not bound by an insurer’s clever drafting and must, nonetheless, interpret such exclusions narrowly because they are exclusions subject to strict construction. In addition, the insurer seeking to avoid coverage based on an exclusion has the burden of persuasion to establish the applicability of the exclusion.

57. The “techno-neutrality” concept was first floated by one of us in the free speech law context. *See generally* Erik S. Knutsen, *Techno-Neutrality of Freedom of Expression in New Media Beyond the Internet: Solutions for the United States and Canada*, 8 UCLA ENT. L. REV. 87 (2001). It is equally apt for insurance law. *See generally id.*

Approaching coverage questions in a techno-neutral way prompts two additional questions. First, what modern enterprise today does not keep electronic records for customers? Second, does this type of coverage prompt policyholders to only keep records in paper form? That would be a silly response that makes little sense. On coverage nullification, and also perverse moral hazard grounds, covering only physical versions of the customer database leads that coverage grant to be an exclusion in sheep's clothing. If it is an exclusion, it should be read narrowly, *contra proferentem* as against the drafter, and should not be permitted to nullify the very coverage it grants.

Taking a techno-neutral approach to insurance coverage questions also helps courts steer clear from time-based analogies that render the jurisprudence unstable and inconsistent. Serious jurisprudential trickle-down effects can occur if a court assesses a certain quality of a cyber loss too early in the life of the technology. For example, a court could find that virtual reality technology is so new and revolutionary that losses arising from its use must be qualitatively different than other losses. Imagine an injury occurring while a participant wears a virtual reality helmet that is projecting the appearance of another digital world to the wearer and the wearer is injured in the physical world by, perhaps, bumping into something that has real substance. Would liability coverage not attach to the helmet manufacturer if it is sued? The technology here is not inherently problematic in bringing about a risk of lawsuits.

Of course, evolution is not revolution and technology changes with time, eventually gets staid, and is itself supplanted by the next latest-and-greatest thing. If a court focuses on the technological novelty of the day, or on the technological mechanics of the policyholder's inherent loss claimed, there is a chance that the interpretive result could be date-stamped and staid in time in relatively short order.

For example, it would be problematic to fixate on an interpretation of a policy term that used a certain vision of the Internet, network security, the cloud, and the World Wide Web as any of these exist at the moment of interpretation. The qualities of paper versus electronic money may be fascinating and almost magical but each is legal tender. Each can be lost, stolen, bartered for, and bargained with. Each is no less "money" than the other. They simply exist in different forms. At an insurance coverage level, treating the loss of electronic funds differently than the loss of paper money simply because of the physicality difference makes little sense.

Where does the techno-neutral approach leave the "electronic data" exclusion, an exclusion so prevalent in liability and property policies? A textualist response to that exclusion would lead a court to exclude from coverage all cyber losses at first blush. The text appears clear on its face:

no coverage for anything related to electronic data or computers. But a trace of the case law shows that courts stretch far to attempt to find coverage for losses by stretching the loss circumstances to include some losses in the physical world that are not caught by the exclusion (for example, the physical inability to use the computer as a circumstance being covered as opposed to the loss of data on it).

We suspect courts are compelled to do this sort of violence to allegedly “clear” text because the exclusion is at odds with a broad coverage grant and the reasonable expectations of modern policyholders who store practically their entire enterprises and personal lives in electronic data form. To hold that the exclusion ousts coverage for only the electronic forms of a loss makes little sense, as we have noted above.

In the insurance law context, there is an argument that the coverage grant is surreptitiously nullified by this surprise exclusion. To be sure, the exclusion makes about as much sense today as saying that only losses involving documents written in a quill pen are covered, whereas ballpoint or typewritten documents are excluded. At a certain point, credulity must snap (even to a textualist response). We think there is, thus, some traction to courts interpreting the exclusion narrowly enough to practically wipe it away as an exclusion that frustrates the very coverage grant of the policy.

This is, in our view, lamentable but not insoluble. There is an alternative scenario—bundling cyber risk into commonly sold property and liability policies. And there is a historical blueprint that insurers can use in the course of achieving this scenario—the development of the CGL policy. Prior to the CGL policy, what we now consider the general liability risks attached to operating a business were insured through a variety of policies, primarily Owners, Landlords, and Tenants Liability, Public Liability Insurance, and Contractors Public Liability Insurance, along with narrower insurance products such as Elevator Liability Insurance, Teams Liability Insurance, Contractual Liability Insurance, and Product Liability Insurance, as well as Owners Protective Liability Insurance and Contractors Protective Liability Insurance. Insurers realized that bundling these separate coverages into a single policy (labeled a “comprehensive” general liability policy before taking on its current “commercial” general liability nomenclature) could be mutually beneficial for policyholders and insurers.⁵⁸

58. See 2 KNUITSEN & STEMPEL, *supra* note 3, § 14.01 (describing the history, development, and evolution of the CGL policy); Jeffrey W. Stempel, *Rediscovering the Sawyer Solution: Bundling Risk for Protection and Profit*, 11 RUTGERS J.L. & PUB. POL’Y 170, 172 (2013) (discussing the particular role of insurance company attorney Elmer Sawyer in the development of the CGL policy and the continued potential for expansion of the standard CGL form and other basic insurance products).

Although it has become a cliché to speak of win-win situations, the CGL actually seems to have accomplished this. Policyholders were able to simplify and streamline their insurance purchasing and have “one-stop shopping” of sorts that reduced policyholder error in failing to purchase sufficiently broad coverage. Insurers were able to encourage broader sales than would have resulted from seriatim sales of narrower policies. The comprehensive policy commanded higher premium payments available to insurers for earning investment income. It also dampened the adverse selection that could occur where policyholders purchased only the coverages they were most likely to draw upon.⁵⁹

The CGL policy has been an economic success for insurers and is generally regarded as generating higher premiums than would have been collected through piecemeal policy sales.⁶⁰ To be sure, the weight of mass torts, such as asbestos and pollution liability claims, has strained the industry at times. But the net negative economic aspect of asbestos claims has been estimated at approximately a three percent reduction in the earnings that would otherwise have been enjoyed by insurers.⁶¹

As the CGL experience reflects, insurers cannot only remain solvent but can profit from bundling risks, even in the face of mass tort pressures. Even serious cyber exposure is unlikely to rival the asbestos crisis already well weathered by the insurance industry. It would appear that cyber coverage could be included in basic property and liability policies without destabilizing risk markets. Or, perhaps more accurately, restrictions on cyber coverage could be removed from basic policies.

We urge a more comprehensive, techno-neutral approach to coverage of cyber losses. We do not argue for economic evisceration of insurers. Surely, some readers will criticize our proposal on the ground that it exposes insurers to excessively large risk if included in core policies and that cyber risk must be separately underwritten and priced to be effective. We strongly disagree and find this objection borderline illogical.

We concede that evaluating cyber risks posed by a particular applicant, and pricing premiums in light of those risks, can be difficult. But the difficulty exists whether this is done in the context of selling a broad-based policy (e.g., all-risk property, CGL, automobile, homeowners) or a stand-alone cyber-risk policy. The same underwriting and pricing that necessarily attends sale of a cyber policy can simply be incorporated into sale of a broader, more comprehensive, core policy.

59. See 2 KNUTSEN & STEMPEL, *supra* note 3, § 14.01.

60. See *id.*

61. See Jeffrey W. Stempel, *Assessing the Coverage Carnage: Asbestos Liability and Insurance After Three Decades of Dispute*, 12 CONN. INS. L.J. 349, 417 (2006).

Narrow, targeted policies may take on less risk but they also do not spread risk by type (although they do spread risk among a pool of policyholders). Regulators recognize this by giving closer scrutiny to the solvency of mono-line insurers compared to multi-line insurers.

The true logic of insurance posits that insurers make money when they are prudent in their underwriting (e.g., not selling policies to suspicious persons or entities engaged in very difficult risks) and pricing (e.g., charging an adequate premium even if this means losing sales to some prospective insurers who are highly (perhaps unduly) price sensitive).⁶² A broad scope of coverage is feasible and can be profitable if priced appropriately. A techno-neutral approach to policy interpretation will help to spur the market towards such a solution by prompting the skittish insurer to draft with an eye to avoiding the pitfalls of techno-centric drafting.

More comprehensive coverage may even reduce the insurer's risk by diversifying the risk. A limited-risk insurer could be devastated if the limited risk becomes a reality because the limited-risk policy was priced entirely on an insulated risk. By contrast, a more broad-based policy that is priced accordingly has risk diversification for the insurer. A given policy year may see unexpectedly high cyber claims—but is unlikely to also see unexpectedly high product liability or trespass or advertising injury claims. Yet the policy was priced based on its comprehensive commitment to coverage that provided the insurer with more premium dollars for investment.

As the example of the CGL policy—which was first widely available in 1941⁶³—illustrates, broad, bundled coverage can benefit both insurers and policyholders. This, in turn, benefits victims through more available compensation and society at large through enhanced

62. Warren Buffett, the CEO of Berkshire Hathaway (“Berkshire”), is one of the world’s richest people. Although Berkshire is best known for (shirts, of course) its consumer brands such as Dairy Queen, Berkshire’s primary business is insurance through its subsidiaries like General Re, National Fire & Marine Insurance Company, and National Indemnity Company. In nearly every one of his famous annual letters to shareholders, which have become staples of the business press, Buffett attributes the success of these insurers (and Berkshire generally) to having sufficient underwriting discipline. *See, e.g.*, Annual Letter from Warren Buffett, Chairman of the Bd., Berkshire Hathaway, Inc., to the Shareholders of Berkshire Hathaway, Inc. 8–13 (Feb. 25, 2017), <http://www.berkshirehathaway.com/letters/2016ltr.pdf>. Buffett prides himself on his insurers’ refusal to write business if it cannot be done at an adequate price. Further, as the experience of other insurers has shown, investment income can often compensate for underwriting loss stemming from underpricing.

63. *See* 2 STEMPER & KNUTSEN, *supra* note 3, §14.01.

socioeconomic stability.⁶⁴ The 80-year history of the CGL policy shows the feasibility of a similar approach to cyber-related risk and loss.

Of course, the easiest solution is to have insurers simply remove exclusions for cyber losses. That would make current policies cyber neutral and, thus, far more streamlined and easier and cheaper to police. But, as mentioned, in the short-term, insurers can enjoy the fruits of a textualist bench now and then by avoiding coverage under this exclusion. That success may well be short-lived, as it only takes one court to “peek” at what is actually going on with the operation of that exclusion before it is read restrictively—or is read out of the policy altogether—as being incongruous with the broad coverage grant and the reasonable expectations of a modern policyholder.

We prefer a market-based solution to the present scope of cyber-loss coverage gaps or, if such is not forthcoming, a market-based solution prompted by courts taking a techno-neutral stance to the interpretation of policy terms covering cyber losses.

While we recognize there may well be some interest in having governmental regulation in the short- to medium-term to help stabilize the coverage landscape for policyholders,⁶⁵ we are confident that the simple pressures of a shift in interpretive approach are enough incentive for insurers to broaden the coverage horizon through simple, targeted revisions to their policies (or alternatively, simple, targeted revisions to courts’ coverage decisions).

As noted, we have seen the insurance market respond to new risk opportunities before and these responses fit the current pattern that is

64. See Erik S. Knutsen, *Auto Insurance as Social Contract: Solving Automobile Coverage Disputes Through a Public Regulatory Framework*, 48 ALTA. L. REV. 715, 716–17, 740–51 (2011) (discussing how insurance coverage issues like auto insurance coverage disputes can be better solved by looking at auto insurance as a “public regulatory document with a public purpose,” whereby the mandatory nature of auto insurance is akin to a “social contract” with society); Jeffrey W. Stempel, *The Insurance Policy as Social Instrument and Social Institution*, 51 WM. & MARY L. REV. 1489, 1494–98 (2010) (noting the importance of insurance to business operations, construction, lending, compensating injured persons, and providing support for development generally).

65. See, e.g., Angela Yu, Note, *Let’s Get Physical: Loss of Use of Tangible Property as Coverage in Cyber Insurance*, 40 RUTGERS COMPUTER & TECH. L.J. 229, 253–54 (2014) (positing that the government may have a role in either mandating cyber insurance coverage or in financially contributing to the current gaps in cyber-loss coverage, until the market is more sustained); see also Kesan & Hayes, *supra* note 17, at 273–76 (canvassing possibilities for government involvement in cyber-loss insurance); Lance Bonner, Note, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL’Y 257, 274–77 (2012) (arguing that the federal government should become more involved in expanding the cyber risk market, as data breaches have become a more pressing problem).

unfolding. To add an additional layer of regulatory uncertainty to the mix would only serve to warp the genesis of the next generation of policies that are destined to provide standard coverage for the plethora of cyber losses facing policyholders today.

Rather than go so far as to mandate (by statute or otherwise) separate coverage⁶⁶ for cyber losses for large institutions like hospitals, banks, and Fortune 500 companies,⁶⁷ we think a simpler solution is to incorporate the coverage into pervasive standard insurance product lines: CGL and commercial property policies, as well as homeowners policies. This can be largely accomplished by a techno-neutral interpretive move in the short- to medium-term. The underwriting effects of such a move would of course have to be sorted out (and costed out) by the providing insurance carriers; however, it is the least intrusive means that still places control of coverage and product pricing in the hands of insurers without necessarily binding the market into an artificially (and inefficiently) segmented world of cyber and non-cyber coverage.

As a corollary, we are not ready to give up regulatory compliance control of cyber losses to the insurance industry either.⁶⁸ Using insurance as an incentive for good cyber-loss risk management produces some questionable results and places a great deal of influence and responsibility on an industry whose incentives are about controlling underlying financial risk to themselves, not necessarily buttressing the societal interests of loss prevention beyond the insurable sphere of a particular insurance policy. The necessary checks and balances for reliable, neutral behavior regulation by insurers are absent in this context, as evidenced by the *Cottage Health Systems* case discussed above, in which insurance coverage for cyber losses was contingent on policyholders adhering to particular data management standards set by insurers (and, dare we say, “for” insurers).

An interpretive approach applying techno-neutrality as the short- to medium-term solution may act as a solid market stabilizer instead of introducing new, untested cyber-specific insurance products. It will at the

66. Whether as drop-down coverage, add-on endorsements to traditional policies, or as separate policies altogether.

67. See Minhquang N. Trang, Note, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches*, 18 MINN. J.L. SCI. & TECH. 389, 389, 412–16 (2017).

68. See, e.g., Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 205–13, 247–48 (2012) (describing how insurers can modify policyholder behavior through *ex ante* coverage requirements); Kesan & Hayes, *supra* note 17, at 268 (“Insurers are in a unique position to push companies to adopt more consistently secure data-security practices”); Shauhin A. Taleh, *Insurance Companies as Corporate Regulators: the Good, the Bad, and the Ugly*, 66 DEPAUL L. REV. 463, 476 (2017) (describing how insurers can act as de facto compliance managers for organizations dealing with cyber security threats).

very least prompt courts to consider the compensatory gaps and coverage nullification issues created as traditional and cyber lines either line up or clash.
