FDCC
QUARTERLY
VOL. 64, NO. 2 WINTER 2015

BROWSE THIS EDITION

FEDERATION OF DEFENSE & CORPORATE COUNSEL

FDCC QUARTERLY

WINTER 2015 VOLUME 64, NUMBER 2

CONTENTS

Cite as: 64 FED'N DEF. & CORP. COUNS. Q. ___ (2015).

The Federation of Defense & Corporate Counsel Quarterly is published quarterly by the Federation of Defense & Corporate Counsel, Inc., 11812 North 56th Street, Tampa, FL 33617.

Coverage Questions Concerning Cybercrimes†

Alan Rutkin
Robert Tugander

I.
Introduction

Insurance coverage law has one firm rule: *When a new risk emerges, new coverage issues follow.*

Cybercrime is a major emerging risk.[1] People use computers in many nefarious ways. Sometimes, the crimes are new and different, such as stealing customer lists, credit card data, or trade secrets. Other times, cybercrimes are new versions of old deeds. Today, bank robbers can use laptops and wifi instead of masks and guns.

In lawyers' eagerness to report on new trends, we sometimes suffer from the "Chicken Little" phenomenon, excitedly addressing concerns that never materialize, such as Y2K. Cybercrime, however, is real.

The headlines make this clear. In August 2014, it was reported that a Russian crime ring stole 1.2 billion usernames and passwords.[2] In 2013, Adobe revealed that hackers stole tens of millions of records.[3] That same year, cyberattacks on retailers such as Target

---

† Submitted by the authors on behalf of the FDCC Insurance Coverage Section.

[1] Danny Yadron, *Police Grapple with Cybercrime*, Wall St. J. (Apr. 21, 2014), http://www.wsj.com/articles/SB10001424052702304626304579508212978109316.

[2] Nicole Perlroth & David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords,* N.Y. Times (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0.

[3] *Id*.

Alan Rutkin, a partner at Rivkin Radler LLP, handles every aspect of insurance coverage law. He has resolved major claims involving the environment, energy, policyholder-owned insurers, and other complex issues. He also assists insurers in writing insurance policies. Mr. Rutkin is the past chair of the ABA TIPS Section's Insurance Coverage Litigation Committee, has held many other ABA leadership positions, and presently serves as one of the elected governors of the TIPS Section. He is a member of the American Law Institute and is currently participating in ALI's project writing the Principles of the Law of Liability of Insurance. Most recently, Mr. Rutkin completed the second edition of The Reference Handbook on the Commercial General Liability Policy. The first edition, published four years ago, was an ABA best seller. Mr. Rutkin is an active member of the Federation of Defense & Corporate Counsel.

and Michael's compromised account information of millions of customers.[4] More recently, some 56 million credit cards may have been compromised in a five month attack on Home Depot.[5]

Statistics tell the story best. In 2013, there were 62% more data breaches than in 2012.[6] Eight of the breaches exposed more than 10 million identities each.[7] In 2013, over 552 million identities were breached.[8] A new risk—cybercrime—has emerged.

Now, insurance coverage issues are emerging. Several factors complicate this body of coverage law.

First, cybercrimes require courts to fit new technologies into old categories. Is data "physical"? Is a data breach a "publication"? How do "intentional act" exclusions apply to computer activity? Courts are wrestling with these and many related issues.

---

[4] Elizabeth A. Harris, *Michaels Stores' Breach Involved 3 Million Customers*, N.Y. Times (Apr. 18, 2014), http://www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html.

[5] Robin Sidel, *Home Depot's 56 Million Cards Breach Bigger Than Target's*, Wall St. J. (Sept. 18, 2014), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

[6] Symantec Corp., Internet Security Threat Report 5 (2014), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[7] *Id*.

[8] *Id*.

Robert Tugander, a partner in the Insurance Coverage & Litigation Practice Group at Rivkin Radler LLP, counsels insurers in complex coverage disputes and represents them in courts across the nation. He handles a wide array of matters relating to environmental, toxic tort, intellectual property, and business tort claims. Mr. Tugander has published several articles on insurance matters and co-authored a chapter in the New Appleman Insurance Law Practice Guide. He is also the co-editor of the Reference Handbook on the Commercial General Liability Policy.

Second, cybercrime-related claims (i.e., "cyberclaims") implicate new and different policy forms. During the last two decades of the 20th century, pollution-related damage raised a host of difficult coverage questions. But these questions generally arose under traditional property or CGL policies and focused on a few common policy terms. Cyberclaims, by contrast, often involve new or different policy forms and novel terms.

Third, computer-specific policies involve factually intensive questions. Policies written to provide coverage for computer-related risks provide specific grants of coverage. Coverage is limited to defined persons, acts, and injuries. These limitations lead to factual disputes.

Given these three factors, as well as the complexity inherent in new technology, difficult coverage issues are emerging. At the time of this writing, courts have decided fewer than forty cyberclaim cases. Most of these cases involve one or more of the following five questions:

1. Does the policy apply to acts by this person?
2. Does the policy cover this act?
3. Does the policy bar coverage because of this person's intent?
4. Does the policy cover this type of injury?
5. Does the policy limit coverage to losses caused "directly" by computer activity?

While the body of case law is still too small to identify trends or majority views, these five questions help organize and understand the existing law.

II.
The Coverage Questions

A. *Does the Policy Apply to Acts by This Person?*

A common coverage question in cyberclaims is whether the policy applies to the acts of the *person* who used the computer to cause the injury.

The issue is authorization. Both *authorized* persons and *unauthorized* persons present risks. But the risks are different, and policies treat them differently. Computer-specific policies often limit coverage to the bad acts of persons who are *not* authorized to use the computer. The issue of authorization has led policyholders to litigate many challenges. In nearly all of the reported decisions, however, insurers have won.

Because computer-specific policies typically exclude acts by employees , the authority issue often focuses on employment status. For example, in *Apps Communication, Inc. v. Hartford Casualty Insurance Co.*,[9] a policyholder sued for coverage under a Computers and Media Endorsement. The endorsement covered physical damage to computer equipment but excluded dishonest or criminal acts by employees.[10] A virus damaged the policyholder's computers, deleting, damaging, or disrupting more than 1,000 files on the computer system and generally disrupting the policyholder's business operations.[11] The policyholder alleged that "a computer virus was introduced" into its computer system, but did not allege who or what introduced the virus. In a decision very favorable to insurers, the court dismissed the policyholder's complaint, ruling that the policyholder's use of the passive voice and absence of detail made the complaint deficient as a matter of law. The policyholder needed to allege who introduced the virus to make it clear that the employee exclusion did not apply.[12]

In *NMS Services, Inc. v. Hartford*,[13] the court reached the same result under what appears to be the same policy form. Again, a policyholder made a claim under a Computer and Media Endorsement to a Special Property Coverage Form.[14] The bad actor, while employed by the policyholder, installed malicious software onto the policyholder's computer system that allowed him to hack into the system after he was terminated and destroy computer files and databases necessary for the operation of the policyholder's business.[15] As in *Apps*

---

[9] No. 11 C 3994, 2011 WL 4905628 (N.D. Ill. Oct. 14, 2011); *see also Palm Hills Props. v. Continental Ins. Co*., No. 07-668-RET-SCR, 2008 WL 4303817 (M.D. La. July 23, 2008) (applying employee exclusion to bar coverage).

[10] *Apps Communication*, 2011 WL 4905628, at *3.

[11] *Id.* at *1.

[12] *Id*. at *3. It is hornbook law that, in general, insurers have the burden to prove the applicability of an exclusion. The effect of the court's ruling in *Apps Communication* was to place the burden on the policyholder to allege facts sufficient to establish that the exclusion did not apply.

[13] 62 F. App'x 511 (4th Cir. 2003).

[14] *Id*. at 512.

[15] *Id*.

Communication, the court ruled that the Endorsement's dishonesty exclusion precluded coverage for the damage.[16]

But that did not mean the policyholder was deprived of coverage altogether. The Special Property Coverage Form itself contained an identical dishonesty exclusion. That exclusion, however, was subject to an *exception*, not found in the Endorsement, which stated that the exclusion did not apply to "acts of destruction by [the policyholder's] employees."[17] Because it was undisputed that the majority of the wrongdoer's bad acts, including installation of the malicious software that allowed destruction of the computer files, occurred while he was an employee, the exception applied, and the policyholder was entitled to coverage in accordance with the provisions of the Special Property Coverage Form.[18]

In addition to exclusions for employee wrongdoing, policies often exclude acts of "authorized representatives."[19] At least two courts have considered and enforced such exclusions.

In *Stop & Shop Cos. v. Federal Insurance Co.*, the First Circuit applied an "authorized representatives" exclusion when a tax payment service stole $55 million from a supermarket.[20] In *Milwaukee Area Technical College v. Frontier Adjusters*, the court applied an "authorized representatives" exclusion when a college's claim adjuster stole $1.6 million.[21]

Three other courts faced more nuanced versions of the authorized persons issue.

In *Universal American Corp. v. National Union Fire Insurance Co*., a "Computer Systems Fraud" rider to a Financial Institution Bond covered "[l]oss resulting directly from a fraudulent . . . entry of Electronic Data . . . into [the policyholder's] proprietary Computer System."[22] The policyholder, a health insurer, suffered over $18 million in losses from fraudulent claims.[23] Most of these claims were submitted by authorized users (providers) who entered fraudulent claim information. The case hinged on the meaning of "fraudulent entry." Did coverage extend to the entry of fraudulent information by authorized users, or was it limited to instances where the entry into the system itself was fraudulent (i.e., unauthorized)? The court, a New York trial court, could not find any New York precedents. Citing decisions from other states, the court found that "entry" unambiguously focused on the act of entering data:

---

[16] *Id.* at 514.

[17] *Id.* at 513.

[18] *Id.* at 513-14.

[19] *See, e.g.,* Stop & Shop Cos. v. Federal Ins. Co., 136 F.3d 71, 72 (1st Cir. 1998) (excluding coverage for loss due to "[t]heft or any other fraudulent, dishonest or criminal act . . . by any [e]mployee, director, trustee or authorized representative of the Insured whether acting alone or in collusion with others").

[20] *Id*. at 72, 76.

[21] 752 N.W.2d 396, 399, 402 (Wis. Ct. App. 2008).

[22] 959 N.Y.S.2d 849, 860 (Sup. Ct. 2013).

[23] *Id*. at 861.

> [T]he Rider states that it covers "fraudulent entry" of data or computer programs into Universal's computer system which resulted in a loss. This indicates that coverage is for an unauthorized entry into the system, i.e. by an unauthorized user, such as a hacker, or for unauthorized data, e.g. a computer virus. Nothing in this clause indicates that coverage was intended where an authorized user utilized the system as intended, i.e. to submit claims, but where the claims themselves were fraudulent.[24]

Because, in the cases before it, the entry of the data was legitimate (even though the data itself was fraudulent), the court found for the insurer.[25]

In *Morgan Stanley Dean Witter & Co. v. Chubb Group of Insurance Cos.*,[26] a New Jersey court faced a similar issue. An authorized person made unauthorized transfers causing about $100 million in losses.[27] Morgan Stanley made claims under an "Electronic and Computer Crime Policy" insuring it "against fraudulent instructions communicated by voice, fax, and computer."[28] The coverage differed depending on the manner by which instructions were given. Where faxes were used, the policy covered only losses from statements that "fraudulently purport to have been made by a customer . . . but which FAX instructions were not made by the customer . . . ."[29] That is, the fax coverage was "imposter coverage," applicable only if the person giving the instruction was not authorized to do so.[30] The voice coverage, however, extended to unauthorized instructions by authorized persons.[31] Consequently, the court found that the fax coverage did not apply, but the voice coverage did apply.[32]

In California, in *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, a federal district court found there was no coverage under a policy covering losses resulting from "Computer Crime" for fraud committed by a payroll company.[33] The payroll company, which was authorized to electronically transfer funds from the insured's account into its own as part of its payroll services, failed to pay the insured's payroll taxes as required by the contract, and instead used the money to pay its own obligations.[34] The insured made a claim

---

[24] *Id.* at 853.

[25] *Id*. at 864.

[26] No. L-2928-01, 2005 WL 3242234 (N.J. Super. Ct. App. Div. Dec. 2, 2005).

[27] *Id*. at *1-2.

[28] *Id*. at *1.

[29] *Id*. at *3.

[30] *Id.*

[31] *Id*. at *5.

[32] *Id*.

[33] No. CV-13-5039-JFW (MRWx), 2014 WL 3844627, at *6-7 (C.D. Cal. July 17, 2014).

[34] *Id.* at *1, 7.

under its Computer Crime coverage, which covered losses directly caused by "Computer Fraud," defined as the "'use of any computer to fraudulently cause a transfer of Money, Securities, or Other Property from inside the Premises or Banking Premises' to a person or place outside the Premises or Banking Premises."[35] According to the court, "Computer Fraud" thus occurs "when someone 'hacks' or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds."[36] Because the payroll company's transfer of funds was authorized and did not involve hacking or any unauthorized entry into a computer system, its acts did not constitute "Computer Fraud." [37] Rather, the fraud took place only after the authorized transfer, and there was no coverage.[38]

In a well-publicized case on a related issue, *Zurich American Insurance Co. v. Sony*,[39] the question was whether the "publication" requirement in a commercial general liability policy's Personal and Advertising Injury coverage was limited to publication by the *policyholder* or extended to publication by *anyone*. The incident giving rise to the litigation was widely reported. Purchasers of Sony's PlayStations gave Sony personal identification, including names, addresses, and credit card data. Hackers breached Sony's system and stole the information. Suits followed. Sony then sought coverage under its Personal and Advertising Injury coverage, which covered injury arising out of "oral or written publication, in any manner, of material that violates a person's right of privacy." According to the court, "publication" meant "publication by the policyholder":

> [The policy] provides coverage only in that situation where the [policyholder] . . . commits or perpetrates the act of publicizing the information . . . . [T]here was no act or conduct perpetrated by Sony, but it was done by third party hackers illegally breaking into that security system. And that alone does not fall under [the invasion of privacy] coverage provision.[40]

Thus, there was no coverage. Sony is appealing.

An Indiana federal court held similarly in *Defender Security Co. v. First Mercury Insurance Co.*[41] Although there was no data breach, the case involved whether there was a

---

[35] *Id.* at *6

[36] *Id.*

[37] *Id*. at *6-7.

[38] *Id*. at *7.

[39] Hearing Tr., No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014) (filed as order Mar. 4, 2014); s*ee N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation*, Ins. J. (Mar. 17, 2014), http://www.insurancejournal.com/news/east/2014/03/17/323551.htm.

[40] Hearing Tr. at 80.

[41] No. 1:13-cv-00245-SEB-DKL, 2014 WL 1018056 (S.D. Ind. Mar. 14, 2014).

publication of an individual's personal information.[42] The plaintiff in the underlying lawsuit against the insured, Defender Security, responded to an ad for home security services by calling a toll free number.[43] She shared personal information with Defender, including her name, address, date of birth, and social security number.[44] She was unaware that the call was being recorded.[45] Plaintiff alleged that Defender's use of call recording technology violated California Penal Code section 632.7, which prohibits the recording of confidential communications made by telephone without the consent of all parties.[46] Defender then sought coverage under the Personal and Advertising Injury provisions of its CGL policy, which required that injury arise from "publication of material that violates a person's right of privacy."[47] The court found there was no "publication."[48] The fact that plaintiff shared personal information during her call, the court reasoned, established at most that plaintiff published information about herself, not that the insured published information about her.[49]

In May 2014, the Insurance Services Office, Inc. (ISO) began introducing endorsements that exclude coverage for claims arising from the disclosure of confidential or personal information. The primary endorsement is CG 21 06 05 14, entitled "Exclusion–Access or Disclosure of Confidential or Personal Information and Data-Related Liability."[50] The current CGL form already has an "Electronic Data" exclusion that excludes coverage for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[51] The new endorsement supplements the existing exclusion by stating that insurance does not apply to damages arising out of "[a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information,

---

[42] *Id*. at *3.

[43] *Id*. at *1.

[44] *Id*.

[45] *Id*.

[46] *Id*.

[47] *Id.* at *2.

[48] *Id*. at *4-5.

[49] *Id.* at *4. *But see Encore Receivable Mgmt., Inc. v. Ace Prop. & Cas. Ins. Co.,* No. 1:12-cv-297, 2013 WL 3354571, at *9 (S.D. Ohio July 3, 2013) (concluding that "publication" occurred "at the very moment that the conversation is disseminated or transmitted to the recording device").

[50] Other endorsements include forms CG 21 07 05 14 and CG 21 08 05 14. CG 21 07 05 14 is identical to CG 21 06 05 14 except that it does not include an exception for Bodily Injury. CG 21 08 05 14 is the same with respect to Coverage B, but there is no replacement exclusion under Coverage A for the Electronic Data exclusion. Similar endorsements have also been introduced for commercial umbrella policies.

[51] *E.g.,* ISO form CG 00 01 04 13, Coverage A, Exclusion p; *see ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, Ins. J. (July 18, 2014), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm [hereinafter *ISO Comments*].

credit card information, health information or any other type of nonpublic information." The exclusion applies to both Coverage A (Bodily Injury and Property Damage) and Coverage B (Personal and Advertising Injury Liability).[52] ISO's explanatory memorandum on the new endorsements states that this is simply a reinforcement of coverage intent—i.e., data breaches and certain data-related liability are not intended to be covered under the CGL form.[53]

B. *Does the Policy Cover This Act?*

In claims arising from cybercrimes, many of the reported cases focus on whether the policy applies to the *act* that caused the injury. The cases address different policy forms with different coverage grants that apply to different factual circumstances. Given the many variables, it is impossible to boil the cases down to a few rules or trends and draw clear lessons. That said, a few points should be noted.

Generally, computer fraud policies cover hacking. Nearly *all* criminals *use* computers. But only *some* criminals *hack* computers. Consequently, a common issue in the "act" cases is distinguishing *hacking* a computer from *using* a computer.

Hacking is "to gain access to a computer illegally."[54] Policyholders have tried to extend hacking coverage to instances in which criminals give bad information that is then legally entered into the policyholder's computer. At least two courts have addressed this scenario. Both courts distinguished giving bad information from actually breaking into a computer, and both courts found that the hacking coverage did not apply.[55]

---

[52] The endorsement further provides that the exclusion will apply even if damages are claimed for notification costs, credit monitor expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by the named insured or other with respect to that which is subject to the exclusion. This endorsement includes a limited Bodily Injury exception arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data. *ISO Comments*.

[53] *Id.*

[54] *Hack Definition*, MerriamWebster.com, http://www.merriam-webster.com/dictionary/hack (last visited Sept. 19, 2014).

[55] Hudson United Bank v. Progressive Cas. Ins. Co., 112 F. App'x 170, 175 (3d Cir. 2004) (loss from fraudulent data entry not covered because data not entered into policyholder's computer); Northside Bank v. Am. Cas. Co., 60 Pa. D. & C. 4th 95, 102 (Ct. C.P. 2001) (coverage protecting bank against hackers did not apply to introduction of information that was fraudulent when received). *See also* Metro Brokers v. Transp. Ins. Co., No. 1:12-cv-3010-ODE, 2013 WL 7117840 (N.D. Ga. Nov. 21, 2013) (policyholder conceded that malicious code and system penetration exclusion applied to virus).

Another issue is that computer fraud policies often require a specific "transfer." Two courts have focused on this issue. In one case, the court did not require a "physical" transfer.[56] In the other, the court found that the transfer must take place from inside the specified premises.[57]

The remaining "act" cases involved fact patterns that seem isolated, if not unique. In one case, a court rejected a policyholder's argument that stealing a computer program could somehow be advertising injury; there was no advertising activity.[58] In three other cases, courts rejected insurers' efforts to apply act-specific exclusions.[59]

C. *Does the Policy Bar Coverage Because of This Person's Intent?*

Closely related to the preceding question about acts is the question of intent. Crime involves bad intent. Thus, the question arises whether intentional act exclusions apply to claims arising from wrongdoing involving computers.[60]

In claims arising from computer crime, courts seem willing to enforce intentional act exclusions.

For example, in *I-Frontier v. Gulf Underwriters Insurance Co.*,[61] an employee stole a manual through use of a computer. The victimized company had coverage for cyberspace activities.[62] The coverage was subject to an exclusion for "any act, error, or omission intentionally committed while knowing it was wrongful."[63] Clearly, the theft was intentional. The court applied the exclusion to bar coverage.[64]

---

[56] Vonage Holdings Corp. v. Hartford Fire Ins. Co., No. 11-6187, 2012 WL 1067694, *3 (D.N.J. Mar. 29, 2012).

[57] Brightpoint, Inc. v. Zurich Am. Ins. Co., No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377, *6 (S.D. Ind. Mar. 10, 2006) (fraudulent transfers not covered because transfer did not move property from inside to outside premises).

[58] Am. States Ins. Co. v. Vortherms, 5 S.W.3d 538, 544 (Mo. Ct. App. 1999).

[59] Retail Ventures, Inc., v. Nat'l Union Fire Ins. Co., 691 F.3d 821, 833 (6th Cir. 2012) (trade secret exclusion did not apply to credit card theft); Netscape Comms. Corp. v. Fed. Ins. Co., 343 F. App'x 271, 272 (9th Cir. 2009) (exclusion for "providing" internet access did not apply); Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co., No. CV095024601, 2010 WL 4226958 (Conn. Super. Ct. Sept. 20, 2010) (counterfeiting exclusion did not apply to email scam).

[60] Many courts have held that "lack of intentionality" is an implicit part of insurance contracts. *See, e.g.*, K&L Homes, Inc. v. Am. Family Mut. Ins. Co., 829 N.W.2d 724, 734 (N.D. 2013).

[61] No. 04-5797, 2005 WL 1353614 (E.D. Pa. June 3, 2005).

[62] *Id*. at *1.

[63] *Id*. at *2.

[64] *Id*. at *3.

Similarly, in *Compaq Computer Corp. v. St. Paul Fire & Marine Insurance Co*.,[65] the policyholder was accused of selling computer drives that were defective.[66] The policy excluded "intentionally wrongful acts."[67] The court held that since the "complaints alleged 'intentional' and 'knowing' conduct . . . the intentional-acts exclusion, as a matter of law, precludes coverage . . . ."[68]

Questions of intent inevitably lead to questions of perspective: From whose perspective is intent considered? This question arose in *Lambrecht & Associates, Inc. v. State Farm Lloyds*.[69] The policy covered "accidental direct physical loss."[70] A hacker disrupted the insured's business.[71] The hacker surely acted intentionally. But whose intent mattered, the hacker's or the policyholder's? The court found that although the hacker intended the injury, the injury was not intended by the policyholder.[72] Because the incident needed to be considered from the policyholder's perspective, the incident was covered.[73]

Also, intentional act exclusions may require substantial evidence. In *Eyeblaster Inc. v. Federal Insurance Co*.,[74] the policyholder was accused of maintaining an internet-based advertising program that disrupted users' computers.[75] The insurer invoked the intentional act exclusion. Certainly, the alleged wrongful conduct seemed inherently intentional. But, the court held, the insurer needed to submit evidence specifically showing that the acts were intentionally wrongful.[76] In the absence of such evidence, the court found for the policyholder and enforced coverage.

D. *Does the Policy Cover This Injury?*

The fourth major dispute concerns whether the policy covers the *injury*. This dispute usually focuses on one of two issues. First, disputes arise whether injuries are "physical" or "tangible" under the policy's Property Damage Liability coverage.[77] Second, disputes

---

[65] No. C3-02-2222, 2003 WL 22039551 (Minn. Ct. App. Sept. 2, 2003). This case addressed intent. But unlike most of the other cases addressed in this Article, the case did not involve acts that were nefarious.

[66] *Id*. at *1.

[67] *Id*.

[68] *Id*. at *5.

[69] 119 S.W.3d 16 (Tex. App. 2003).

[70] *Id*. at 18.

[71] *Id*.

[72] *Id*. at 22.

[73] *Id*.

[74] 613 F.3d 797 (8th Cir. 2010).

[75] *Id*. at 799.

[76] *Id*. at 804.

[77] "Property damage" is typically defined as "physical injury to tangible property" or "loss of use of tangible property that is not physically injured."

arise as to whether injuries constitute "Personal Injury" as defined in the policy's Personal and Advertising Injury Liability coverage.

Even though digital data differs from our view of "physical," policyholders have often succeeded in arguing that data is "physical."

Several policyholders established "physical" damage by tying data to hardware. For example, in *Eyeblaster Inc. v. Federal Insurance Co.*, the Eighth Circuit held that a frozen computer constituted a loss of use of tangible property.[78] There, the court focused on the computer itself to find something physical.[79]

Similarly, in *Vonage Holdings Corp. v. Hartford Fire Insurance Co.*,[80] the court found a loss to be insured by focusing on the lost ability to use full capacity of servers.

Finally, in *Lambrecht v. State Farm*,[81] the court again focused on hardware to find something "physical." The insurer argued that loss of information was not "physical" because it did not exist in a physical form. The court, however, found that the loss was "physical" because it affected the server, which had a hard drive that could not be used.[82]

In *Landmark American Insurance Co. v. Gulf Coast Analytical Laboratories*,[83] the court did not focus on the hardware; it focused purely on the data. This focus should have favored the insurer, but the policyholder still won. The *Landmark* court held that:

> [T]angibility is not a defining quality of physicality according to Louisiana law. The Louisiana Supreme Court determined that though electronic data is not tangible it is still physical because it can be observed and altered [through] human action. Therefore, according to Louisiana law, GCAL's electronic chemical analysis data must be considered a corporeal movable or physical in nature. Therefore . . . GCAL's electronic data "has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and *can be perceived by the senses*." Since

---

78 613 F.3d at 802.

79 *Id*.

80 2012 WL 1067694, at *3.

81 119 S.W.3d 16 (Tex. App. 2003).

82 *Id*. at 23. Outside of the crime context, courts have reached different conclusions about whether data is tangible. For example, in *America Online, Inc. v. St. Paul Mercury Ins. Co.,* 347 F.3d 89, 95 (4th Cir. 2003), the court held that lost data is not "physical damage to tangible property." But, the court held, "if a hard drive were physically scarred or scratched so that it could no longer properly record data . . . then the damage would be physical . . . ." On the other hand, another court found that "'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." Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185 TUC AM, 2000 WL 726789, at *2 (D. Ariz. Apr. 18, 2000).

83 No. 10-809, 2012 WL 1094761 (M.D. La. Mar. 30, 2012).

> the GCAL's electronic data is physical in nature under Louisiana law, summary judgment is appropriate, declaring that electronic data is susceptible to "direct, physical 'loss or damage.'"[84]

It seems unlikely that the *Landmark* court's analysis will gain broad acceptance. First, the case was decided under Louisiana's civil law conception of "corporeal movable property," which the court itself noted differed from the common law interpretation.[85] Second, the court's analysis simply does not withstand scrutiny. While it was appropriate for the court to consider physicality as being "perceived by the senses"—in fact, "physical" is defined as "existing in a form that you can touch or see"[86]—you cannot "touch or see" digital data.

In fact, in a case on a related issue, *Carlon Co. v. DelaGet*, LLC,[87] the court found for the insurer. The policyholder was sued for negligence in safeguarding a bank passcode, which allowed money to be removed from a customer's bank account. The court held there was no property damage coverage because electronic bank account funds were not "tangible property."[88]

The question whether computer crimes constitutes "Personal Injury" within the meaning of Personal and Advertising Injury Liability coverage has also been the source of litigation. Here, insurers and policyholders have both enjoyed victories, leaving no clear law.

With respect to the invasion of privacy offense—e.g., "oral or written publication, in any manner, of material that violates a person's right of privacy"—a key question is whether a "publication" has occurred. In the computer crime context, this question is complicated. Is there "publication" once the thief acquires the information, or does "publication" require something more? Again, courts disagree. At least one court has found that the acquiring of information is not in itself a publication.[89] But another court, interpreting a policy that required "making known" the information (as opposed to "publication"), the court held that intercepting and internally disseminating messages is "making known" the information.[90] In so holding, the court found the policy's language covering disclosure to "any" person or organization to be dispositive.

---

[84] *Id.* at *4 (emphasis added).

[85] "The Louisiana Civil Code departed from the narrow Roman law conception that only 'tangible objects' were corporeal; instead, 'the Louisiana Civil Code of 1870 declared that perceptibility by any of the senses sufficed for the classification of a material thing as corporeal.'" *Id.* at *3.

[86] *Physical Definition*, Merriam-Webster.com, http://www.merriam-webster.com/dictionary/physical (last visited Sept. 19, 2014).

[87] No. 11-CV-477-JPS, 2012 WL 1854146 (W.D. Wis. May 21, 2012).

[88] *Id*. at *4.

[89] Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664, 672-73 (Conn. App. Ct. 2014).

[90] Netscape Comms. Corp. v. Fed. Ins. Co., 343 F. App'x 271, 272 (9th Cir. 2009).

Beyond the cases concerning the definition of "physical" and the scope of "Personal Injury" coverage, several cases address the characterization of the insured's loss. In *Retail Ventures, Inc. v. National Union Fire*, the Sixth Circuit rejected an insurer's effort to treat credit card information as "trade secrets," and thus held a trade secrets exclusion did not apply.[91] In *Royal American Group v. ITT Hartford*, the court rejected a policyholder's attempt to characterize distance telephone services as "securities," and thus held these services were not "covered property" (a term defined to include "securities").[92]

E. *Does the Policy Limit Coverage to Losses Caused "Directly" by Computer Activity?*

Claims under computer policies typically limit coverage to "direct losses" from, or "loss resulting directly from," specified computer-related misconduct. Thus, these claims frequently raise causation issues.

Insurers often argue that "direct means direct."[93] At a minimum, insurers maintain that direct means immediate, without an intervening cause. Policyholders, on the other hand, argue for a "proximate cause" approach.

In *Owens, Schine & Nicola, P.C. v. Travelers Casualty & Surety Co.*[94] and *Retail Ventures, Inc. v. National Union Fire Insurance Co.*,[95] criminals used computers to gain access to their victims. In *Owens*, the criminal solicited the victim by email, and then once in contact, defrauded the victim. In *Retail Ventures*, the criminals used computers to steal credit card information, and then stole from the accounts. In other words, the computers were used to set up the crimes, but the computers were not used to effectuate the crimes. Both courts found the losses resulted directly from computers.

On the other hand, several courts have found that the use of a computer was merely incidental to the loss and thus not covered. In *Pinnacle Processing Group v. Hartford Casualty Insurance Co.*,[96] the court held that "direct" means "without any intervening cause." In *Brightpoint, Inc. v. Zurich American Insurance Co.*,[97] the court cited *Black's Law Dictionary* to state that direct means "[i]n a straight line or course" and "immediately."[98] In *Pestmaster*,

---

91 691 F.3d 821, 833 (6th Cir. 2012).

92 No. 16246, 1994 WL 14888, *2-3 (Ohio Ct. App. Jan. 12, 1994).

93 *See, e.g.,* Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821, 828-29 (6th Cir. 2012) (collecting cases).

94 No. CV095024601, 2010 WL 4226958 (Conn. Super. Ct. Sept. 20, 2010).

95 691 F.3d 821.

96 No. C10-1126-RSM, 2011 WL 5299557, at *5. (W.D. Wa. Nov. 4, 2011).

97 No. 1:04-CV-2084-SEB.-JPG, 2006 WL 693377 (S.D. Ind. Mar. 10, 2006).

98 *Id.* at *7.

the court stated, "direct means direct," and held that losses must "flow immediately and directly" from computer use.[99]

In *Metro Brokers, Inc. v. Transportation Insurance Co.*, the court took a broader view of causation based on policy language excluding loss "caused directly or indirectly" by "malicious [computer] code" or "system penetration."[100] Thieves used a computer virus to steal a bank customer's login and password information, then accessed the bank's online banking system and transferred money from the customer's accounts to other accounts in the thieves' control.[101] A dispute arose as to whether the policy's virus exclusion applied.[102] The policyholder argued that the exclusion did not apply because the virus was not the "cause" of the loss; rather, the loss was caused by the actions of humans using information obtained by the virus.[103] Because the exclusion applied to any loss "caused directly *or indirectly*" by a virus, the causation requirement was relaxed.[104] Moreover, the exclusion applied "regardless of any other cause or event that contributes concurrently or in any sequence to the loss."[105] Thus, the court ruled, "[t]he virus's contribution to this particular loss is not too remote to fall outside the parameters of proximate causation contemplated" by the policy.

Insurers won two other causation cases, but both cases show that computer fraud coverage requires more than a criminal using a computer; the criminal must use the computer to cause the fraud. In *Great American Insurance Co. v. AFS/IBEX Financial Services, Inc.,*[106] an insurance agent used a computer to file false insurance premium financing applications with AFS/IBEX, which then sent send premium checks to the agent, who deposited them in his own account. According to the court, the loss was not covered because it did not "directly stem[] from fraud perpetrated by use of a computer," as required by the policy.[107]

In *Methodist Health System Foundation, Inc. v. Hartford Fire Insurance Co.*,[108] the insured invested in a mutual fund that invested in a hedge fund that in turn invested with Bernard Madoff. The insured suffered losses from its investment portfolio after Madoff's Ponzi scheme was discovered and sought coverage for these losses under a commercial crime

---

[99] *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co.,* No. CV-13-5039-JFW (MRWx), 2014 WL 3844627, at *7 (C.D. Cal. July 17, 2014) (computer was merely incidental to misuse of funds where fraud occurred after an authorized electronic transfer).

[100] No. 1:12-CV-3010-ODE, 2013 WL 7117840, at *1 (N.D. Ga. Nov. 21, 2013).

[101] *Id*. at *2.

[102] *Id*. at *2-3.

[103] *Id*. at *2.

[104] *Id.* at *5 (emphasis added).

[105] *Pestmaster*, 2014 WL 3844627, at *5.

[106] No. 3:07-CV-924-O, 2008 WL 2795205 (N.D. Tex. July 21, 2008).

[107] *Id.* at 14.

[108] 834 F. Supp. 2d 493 (E.D. La. 2011).

policy. The court rejected this claim: "[W]hile the Madoff ponzi scheme was a contributing factor in Plaintiff's sustained losses, [it] was not a direct cause of Plaintiff's losses" as required by the policy.[109] The loss was "too many steps removed from Madoff's fraud"[110] and thus was not covered.

Much like causation cases in the tort context, the causation cases here are difficult to reconcile. Four courts have addressed this issue, with insurers winning two and policyholders winning two. Moreover, insurers won the two cases with the tighter causal chain; courts found the chain too attenuated to establish causation. Policyholders won the two cases with the weaker causal chain; courts found the chain adequate to establish causation.

One possible explanation is that "proximate cause" is a relaxed standard. Three of the courts that found for policyholders adopted the "proximate cause" approach.[111] Nonetheless, it is unclear that "proximate cause" means something different from the terms that courts used in finding for insurers.

III.
Conclusion

Since fewer than forty courts have addressed insurance coverage for criminal conduct, it is too soon to draw firm conclusions. But the five issues discussed here seem likely to recur.

The coverage disputes may extend to other issues. In fact, the cases concerning cybercrime do address a few other issues. Some of these issues are specific to computers.[112]

---

[109] *Id.* at 496.

[110] *Id*. at 497.

[111] *See* Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co., No. CV095024601, 2010 WL 4226958 (Conn. Super. Ct. Sept. 20, 2010); Retail Ventures, Inc., v. Nat'l Union Fire Ins. Co., 691 F.3d 821, 831-32 (6th Cir. 2012)*;* Transtar Elec., Inc. v. Charter Oak Fire Ins. Co., No. 3:13cv1837, 2014 WL 252023, at *4 (N.D. Ohio Jan. 22, 2014).

[112] *See, e.g.,* I-Frontier, Inc. v. Gulf Underwriters Ins. Co., No. 04-5797, 2005 WL 1353614, at *3 (E.D. Pa. June 3, 2005) (declining to "delve into the interpretation of the term 'cyber-space activities'"); Eyeblaster Inc. v. Fed. Ins. Co., 613 F.3d 797 (addressing application of intellectual property exclusion); Nationwide Ins. Co. v. Hentz, No. 11-cv-618-JPG-PMF, 2012 WL 734193, at *6 (S.D. Ill. Mar. 6, 2012) (addressing application of care and custody exclusion to stolen laptop); Hewlett-Packard Co. v. Factory Mut. Ins. Co., No. 04 Civ. 2791 (TPG)(DCF), 2007 WL 983990, at *2-3 (S.D.N.Y. Mar. 30, 2007) (excusing insured's late notice of claim based on delayed discovery of computer sabotage).

Other coverage cases involving cybercrime seem to hinge on insurance issues that are not computer-centric.[113]

Ultimately, since these claims are brought under specifically tailored policy provisions, these factually intensive coverage disputes will continue to arise.

[113] Freedom Banc Mortg. Servs., Inc. v. Cincinnati Ins. Co., No. 13AP-400, 2014 WL 294655, at *1 (Ohio Ct. App. Jan. 23, 2014) (analyzing time limit on suit); Pollak v. Fed. Ins. Co., No. 13-12114-FDS, 2013 WL 6152335, at *4 (D. Mass. Nov. 21, 2013) (interpreting "intended beneficiary"); Saint Consulting Grp., Inc. v. Endurance Am. Specialty Ins. Co., No. 11-11279-GAO, 2012 WL 1098429, at *3 (D. Mass. Mar. 30, 2012) (addressing application of exclusion for statutory violations).

The Federation of Insurance Counsel was organized in 1936 for the purpose of bringing together insurance attorneys and company representatives in order to assist in establishing a standard efficiency and competency in rendering legal service to insurance companies, and to disseminate information on insurance legal topics to its membership. In 1985, the name was changed to Federation of Insurance and Corporate Counsel, thereby reflecting the changing character of the law practice of its members and the increased role of corporate counsel in the defense of claims. In 2001, the name was again changed to Federation of Defense & Corporate Counsel to further reflect changes in the character of the law practice of its members.

The FEDERATION OF DEFENSE & CORPORATE COUNSEL QUARTERLY, published quarterly through the office of publication by the Federation of Defense & Corporate Counsel, Inc., 11812 North 56th Street, Tampa, FL 33617.

Manuscripts and correspondence relating to the submission of articles for possible publication should be sent to the Editor-in-Chief, Susan M. Popik, 38 Woodhill Drive, Redwood City, CA 94061 or emailed to susan.popik@thomsonreuters.com. All other correspondence should be directed to the Executive Director.

The FDCC is pleased to provide electronic access to Quarterly articles from 1997 to present at its Internet website, www.thefederation.org.