Insurance Disputes Over Cyber Claims

Current and Future Flashpoints

by Robert D. Chesler and Christina Yousef

The world of cyber-insurance remains in flux. More than 60 insurance companies are now offering cyber-insurance policies, with no standardization or uniformity. Such an array of policies places a heavy burden on insurance professionals as they try to locate the best language in an area where even a minor mistake in wording can be disastrous.

Moreover, precious little guidance exists. Only one case substantively addressing a term in a cyber policy has appeared to date. This may be a good thing—anecdotally, insurance companies are paying claims under these policies, accounting for the lack of litigation. Whether this remains the case is yet to be seen. Many insurance coverage attorneys predict a wave of cyber-insurance litigation in the future.

Junk Fax Litigation

The place to start with an examination of cyber-insurance litigation is the continuing onslaught of Telephone Consumer Protection Act[1] (TCPA) claims. These are known as junk fax claims; they arise from the unsolicited faxes people used to receive in great quantities. TCPA set a fine of $100 for each individual fax sent without permission. This created a tremendous incentive for lawyers to sue the senders of junk faxes. Moreover, even when it was a tiny company that sent out the fax, it might still have millions of dollars of insurance coverage. There are well over 50 decisions on insurance coverage for junk fax claims.

The basic issue in this litigation is the meaning of the word 'privacy.' The typical personal injury section of a general liability policy provides coverage for injury arising out of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." Insurance companies assert that two types of privacy exist. The first is solitude—the right to be left alone. This, insurance companies argue, would be the type of privacy impinged by junk faxes. The second type of privacy is secrecy, the freedom not to have one's secrets communicated to a third party. Since the insurance policy used the term 'publication,' insurance companies asserted that the privacy coverage in the insurance policy only applied to secrecy and not to solitude, and, therefore, did not provide coverage for junk faxes. That is, violating people's privacy via publication suggests exposing their secrets.

This issue has been fought out in dozens of states, with policyholders generally holding the advantage. The only case in New Jersey is an unpublished trial court decision. The court, in *Myron Corp. v. Atlantic Mutual Ins. Co.,* held that the insurance company had a duty to defend.[2] The court found that the right of privacy encompassed both secrecy and seclusion, and that coverage was within the policyholder's objectively reasonable expectations.[3]

It was not long before the insurance companies added junk fax exclusions to new general liability insurance policies, canceling out the possibility of coverage for junk fax liability going forward. However, a second area of cyber litigation commenced under general liability policies—coverage for data breaches.

Data Breach Cases

In *Total Recall Info. Mgmt. v. Federal Ins. Co.*, computer tapes literally fell off the back of a truck.[4] When the company went back to retrieve the tapes, which contained sensitive personal information, they had vanished. There was no evidence the tapes were ever accessed, and Recall Total spent over $6,000,000 trying, unsuccessfully, to recover them.[5]

Recall Total sought to recover its cost from its general liability insurance company, under the same 'privacy' provision in the insurance policy as was at issue in the junk fax coverage litigation. Here, though, the key word was 'publication.' The Connecticut Supreme Court held that if there was no access to

the information, no publication took place. The court denied coverage.[6]

Travelers Indemnity Co. v. Portal Healthcare Solutions reached the opposite conclusion.[7] In this case, personal medical information was placed on the Internet. However, no one accessed the information. The district court found that regardless of whether anyone had accessed the information, it was still published. The court held that "Publication occurs when information is 'placed before the public,' not when a member of the public reads the information placed before it."[8] Thus, the court held that general liability policies provided coverage for data breaches.[9]

It did not take the insurance industry long to develop an exclusion for data breaches for the general liability policy. In 2014, the industry released a massive data breach exclusion that stated, in part, that liability "arising out of any access to or disclosure of any person's or organization's confidential or personal information" was excluded from coverage.[10] This exclusion conclusively established that the general liability policy did not provide coverage for data breach in any form.[11] Policyholders would need to seek coverage under other types of policies.

The lesson from the junk fax and data breach cases is that the insurance industry will move rapidly to remove new liabilities from coverage under the general liability policy. This was true for environmental liability, mold and, largely, intellectual property. In each case, policyholders had to look to new policies for coverage.

Directors and Officers (D&O) Policies

Before turning to computer coverage and cyber policies, it is necessary to address D&O policies. Data breaches have given rise to shareholders' derivative suits against directors and officers. Normally, D&O policies should protect against such suits. However, some D&O policies contain privacy exclusions. These exclusions probably originated because general liability policies covered privacy; however, that is no longer the case. These exclusions may block coverage for directors and officers sued by shareholders over a data breach. Insurance professionals should make sure that D&O policies do not contain such exclusions. If they do, the company needs to purchase a cyber policy that provides such coverage.

Miscellaneous Computer Coverage

A number of insurance policies now provide limited computer coverage, either by endorsement or within the body of the policy. Such policies include crime policies, bankers' policies, and executive risk policies. Two issues have arisen under these policy provisions. First, insurance companies have contended that certain losses were not 'direct,' as required by the policy. Second, insurance companies have asserted that while the policies provide coverage for hacking—an outside party breaking into a company's data—they do not provide coverage for phishing—fraudulently inducing a company insider to expose data or transfer funds.

The most recent case in this area is *Principle Solutions Group v. Ironshore Indemnity*.[12] *Principle* concerned a commercial crime policy that provided coverage for loss "resulting directly from a 'fraudulent instruction….'"[13] Principle lost $1,717,000 in a phishing scam that included several steps after the initial phone call impersonating the company's president.[14] Principle argued that the loss was direct, while Ironshore asserted the intervening factors made it indirect.[15] The court found both explanations reasonable, and concluded that an ambiguity existed.[16] As a result, the court held for Principle.[17]

State Bank of Bellingham v. BancInsure reached a similar conclusion. *Bank of Bellingham* concerned a financial institution bond that covered computer system fraud.[18] A secretary left a computer on overnight, resulting in the hacking of the computer system. The court found coverage, holding that the hacking was the efficient proximate cause of the loss.[19]

Policyholders have fared less well on the hacking versus phishing controversy. *Universal American Corp. v. National Union Fire Ins. Co. of Pittsburgh, Pa.* concerned computer coverage in a financial institution bond.[20] The policy provided coverage for "fraudulent entry" into a computer system. The court found this coverage was limited to hackers, and not to fraudulent content submitted by authorized users.[21]

The Fifth Circuit recently denied coverage in *Apache Corp. v. Great American Insurance Co.*, which involved computer coverage in a crime policy that provide for "loss...resulting directly from the use of any computer…."[22] *Apache* was a phishing case where the phisher sent a fraudulent email to a secretary. She showed it to another employee, who showed it to a supervisor. The company honored the email and lost $2,400,000. The trial court found the loss resulted directly from the computer.[23] The Fifth Circuit reversed, finding that every fraud that happened to use a computer did not qualify as a computer fraud.

Several similar cases are currently pending.[24]

Cyber-Insurance Policies

P.F. Chang's v. Federal Insurance Co. is the first judicial decision on a cyber-insurance policy.[25] In that case, a hacker accessed 60,000 records. The insurance company positively responded to the resulting claim, at least in part. It paid $1,700,000 to conduct a forensic investigation and to defend litigation.[26] However, the insurance policy had a contract exclusion, and the insurance company refused to pay for what it characterized as a contract claim.[27] As a vendor, Chang

was not permitted to deal directly with banks, and used middlemen, with whom it had a contract.[28] Chang's servicing bank charged about $1,900,000 in penalties and fees to the middleman as a result of the breach, and the middleman passed the charge over to Chang, pursuant to their contract.[29] The court denied coverage for this claim based on contract exclusions in the insurance policy.[30] The case is currently on appeal.

Ten Tips When Writing Cyber-Insurance Policies

1. *Eliminate or limit contract exclusions*. As shown by *Chang*, too much of cyber exposure is related to contractual obligations to safely allow a broad contract exclusion in cyber policies.
2. *Make the policy understandable*. Cyber policies have dozens of cross-referenced, multi-part definitions and exclusions that make the policy extremely difficult to understand. Work with an insurance professional to track through the policy to make sure the coverage needed is provided.
3. *Watch out for evolving risks*. The world of cyber risks changes rapidly. Now, a major concern is ransomware, which was little noticed two years ago. Make certain the policy adapts to these changes.
4. *Eliminate or limit retroactive dates*. A retroactive date means events that took place prior to that date are not covered. Many data breaches remain undiscovered for an extended period of time. Policies should either eliminate retroactive dates or have the earliest date possible.
5. *Avoid cybersecurity 'reasonableness' clauses*. The policy should not have a requirement that the policyholder maintain 'reasonable' cybersecurity measures; what is reasonable changes rapidly over time.
6. *Watch out for sub-limits*. It is possible to believe, for example, one has a $1,000,000 policy, only to find that sub-limits dramatically reduce key coverages.
7. *Have coverage for third parties, including vendors*. Many data breaches are caused by the actions of vendors, including cloud vendors. Coverage should be included for this exposure.
8. *Limit war exclusions*. Keep these as narrow as possible. Is a cyber attack from North Korea excluded?
9. *Watch out for exclusions for consumer protection laws*. This is a significant exposure that should be covered.
10. *Is there coverage for fines and penalties?* Much of a company's exposure for a data breach stems from fines and penalties levied by government entities. This is an essential coverage element. It is also a good example of a coverage that can be included but reduced by inadequate sub-limits. ⚖

Robert D. Chesler *is a shareholder and* ***Christina Yousef*** *an associate in the insurance recovery group at Anderson Kill, P.C., practicing in the firm's Newark office.*

ENDNOTES

1. 47 U.S.C. § 227.
2. N.J. Super. Unpub. Lexis 3012 (Law Div. 2007).
3. *Id*. at *16.
4. 115 A.3d 458 (2015).
5. *Recall Total Info. Mgmt. v. Fed. Ins. Co*. 83 A.3d 664, 668 (Conn. App. Ct. 2014).
6. *Id*. at *50-51.
7. 35 F. Supp. 3d 765 (E.D. Va. 2014), *aff'd*, 2016 U.S. App. Lexis 6554 (4th Cir. 2016).
8. *Id*. at 771.
9. *Id*. at 769.
10. Insurance Services Office, *see* form CG21070514.
11. *Id*.
12. No. 1:15-CV-4130 (RWS), 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).
13. *Id*. at *2.
14. *Id*. at *1-2.
15. *Id*. at *4.
16. *Id*. at *5.
17. *Id*.
18. 823 F.3d 456 (8th Cir. 2016).
19. *Id*. at 461.
20. 37 N.E.3d 78 (N.Y. 2015).
21. *Id*. at 81.
22. No. 15-20499, 2016 WL 6090901, at *2 (5th Cir. Oct. 18, 2016).
23. *Apache Corp. v. Great Am. Ins. Co*., No. 4:14-CV-237, 2015 WL 7709584, at *3 (S.D. Tex. Aug. 7, 2015), *vacated*, No. 15-20499, 2016 WL 6090901 (5th Cir. Oct. 18, 2016).
24. *See*, *e.g.*, *Medidata Solutions, Inc. v. Federal Insurance Company*, No. 1:15-cv-907 (ALC) (S.D.N.Y. filed Feb. 6, 2015).
25. 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 26, 2016).
26. *Id*. at *5.
27. *Id*. at *21.
28. *Id*. at *3-4.
29. *Id*. at *6-7.
30. *Id*. at *29.