This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

3

"THE HACKERS DID THIS": DATA BREACH LAWSUITS AND COMMERCIAL GENERAL LIABILITY INSURANCE

In April 2011, Sony's popular PlayStation Network was compromised and intruders stole information about seventy-seven million PlayStation users' accounts, including their names, addresses, email addresses, birthdays, usernames, passwords, security questions, and credit card numbers. It was one of the largest data breaches ever reported at the time and Sony customers quickly filed a series of lawsuits against the company for failing to protect their personal data, and several of those lawsuits were combined into a class action complaint. Although many of the class action plaintiffs' claims were dismissed in 2012 by district judge Anthony J. Battaglia because Sony had warned customers explicitly in its privacy policy that "there is no such thing as perfect security,"[1] the class action suit ultimately cost Sony nearly $18 million, including a $15 million settlement reached in July 2014 and $2.75 million in legal fees.[2] Faced with these mounting legal fees, Sony looked beyond its data breach insurance to its commercial general liability (CGL) insurance to help cover its legal costs. CGL policies in the United States date back to 1940 and offer coverage for both legal fees and damages related to lawsuits brought against the policyholders for bodily injury or property damage.[3] In the decades following their initial development, CGL policies expanded to cover additional types of risks, such as liability for advertising and privacy harms related to issues including slander, copyright infringement, or misappropriation of someone's name or likeness. Sony hoped that it might be able to claim the 2011 breach as a type of privacy harm through its CGL policy with Zurich American Insurance. Zurich and Sony's other insurers, including the Mitsui Sumitomo Insurance Company of America, vehemently disagreed, pointing to the wording of Sony's policy, which had clearly been drafted with a very different sort of privacy harm in mind. Ultimately, that language would help Zurich and other insurers prevent policyholders like Sony from exercising CGL policies to cover legal costs related to most data breaches. This, in turn, contributed to the trend of carriers

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

shifting cyber risks into their own cyber-specific policies rather than integrating them into existing product lines and categories of risk.

More was at stake in the dispute between Sony and Zurich than just the question of who would end up covering Sony's legal fees. The case raised complicated questions about cybersecurity liability and who was at fault when a data breach occurred—the hackers who instigated the breach or the business that failed to defend itself against intrusion. Those questions were also central to the class action suit against Sony that played out in parallel to the company's dispute with Zurich, and the two cases put Sony in the complicated position of arguing simultaneously that it was entirely at fault for the breach (and therefore justified in exercising its CGL policy) and that it was not to blame in the least because it had been the unfortunate victim of malicious hackers. Beyond its implications for who bore the most responsibility for data breaches, the fight between Sony and its insurers also mattered because it was the first lawsuit that dealt with the question of whether CGL policies covered liability related to data breaches. Most CGL policies were relatively standardized across insurers because their language had been drafted by the Insurance Services Office, so if the language in Sony's policy from Zurich was interpreted as covering data breach liability, that would likely mean that many other CGL policies would be similarly applicable to breaches. On the other hand, if CGL policies did not cover data breaches, that would make it all the more urgent for companies to invest in separate, breach-specific policies of the sort that had begun to be sold in the late 1990s and early 2000s but had not by any means become routine purchases by 2011, when the Sony breach occurred. Sony, in fact, did have data breach insurance at the time of its breach—but the coverage was presumably less than the company felt it needed to pursue litigation and cover the potential damages. If it turned out they could supplement that coverage with their CGL coverage, it might be enough to see them through. Otherwise, the lesson for them and others would be not just to purchase breach insurance, but to buy lots of it.

For insurers, the case was therefore important not just as a way to protect the limits of their existing CGL coverage, but also as a way to potentially expand the market for a new product that could generate more customers and revenue. Both insurers and insurance customers had long understood that creating a market for a new class of insurance would require insurers to carve coverage for those types of risks out of their existing policies. Indeed,

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

in a piece about cyberinsurance in the *Long Island Business News* in 2001, a decade before the Sony breach, Ty Sagalow, the chief operating officer of AIG's eBusiness Risk Solutions group, is quoted as warning businesses that "any company that does business via computers may not be covered by traditional business insurance" and that they should buy a cyber-specific policy.[4] Later that same year, an article in *Forbes* about computer risk insurance noted, "What's pushing companies into these policies is the fear that insurers will begin specifically striking hack-related coverage from general property and casualty policies once claims begin escalating, just as they did in the 1990s with sexual harassment, discrimination and pollution liabilities." The article quotes a risk manager at a bank who was, at the time, negotiating the purchase of $75 million of "hacker coverage" from Chubb, predicting "what I see coming down the road is a sort of Internet exclusion."[5]

NEGLIGENT CYBERSECURITY AND LIABILITY FOR DATA BREACHES

While breach notification laws had made it easier to sue companies for failing to protect their customers' personal information, the liability regimes governing these incidents were still far from clear in 2011, when the Sony PlayStation breach occurred. The dismissal of several data breach class action lawsuits, including one brought against Barnes & Noble for a 2013 breach of customer payment card numbers at sixty-three stores, illustrated that just because individuals were now being notified of breaches affecting their personal information did not mean breached companies were all of a sudden facing massive new liabilities. But neither could companies be confident that they wouldn't be held liable for these incidents. There was no clear set of security standards or requirements that they could point to and say they had complied with to absolve themselves of responsibility for breaches—in other words, nobody was certain what constituted negligence when it came to cybersecurity. On top of that, many data breaches and other types of cybersecurity incidents involved multiple different, interconnected entities. Software and hardware manufacturers, website designers and hosts, payment processors and Internet service providers might all play some role in enabling breaches by leaving vulnerabilities in code, for instance, or failing to detect and block criminals operating on their infrastructure. Deciding who to blame was far from straightforward and depended a great deal on the particular details of any given incident.[6]

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

For the software and hardware industry, the liability issue was very straightforward—they had been absolved of any liability for vulnerabilities or security issues in their products under the Computer Fraud and Abuse Act (CFAA) passed in 1986. Lobbyists had argued over and over to Congress that it was impossible to develop bug-free code and any attempt to hold tech firms liable for those bugs would destroy the industry altogether, prompting the liability protections in the CFAA. But firms that were not hardware or software companies had no such liability shield when it came to their failures to protect data or computer networks. Still, the risks of being held liable for such breaches did not seem to dissuade firms from collecting and storing digital data on their customers. In fact, the impossibility of implementing perfect security provided firms with a possible means of defending themselves from liability for security breaches: they could just say, truthfully, that there was no sure-fire way of preventing such incidents.

The consolidated class action complaint filed against Sony in California in 2012 alleged that Sony had not even maintained "reasonable, adequate and industry-standard security measures," and that the PlayStation Network "lacked basic security measures such as updated software, adequate encryption and firewalls." Though these measures were not specifically required by law, the plaintiffs claimed they had been deceived by Sony's privacy policies, which promised that the company took "reasonable measures to protect the confidentiality, security, and integrity" of customers' personal information, even as it cautioned users that "there is no such thing as perfect security." The problem was not Sony's failure to perfectly secure its networks, the plaintiffs alleged, but instead the company's failure to live up to the promises of its own privacy policy that personal information would be "stored in secure operating environments that are not available to the public" and that the company would "use industry-standard encryption" to protect "sensitive financial information" such as credit card numbers. In reality, the story was more complicated. The company had encrypted customer credit card numbers, but it had failed to encrypt other information about its customers, including their passwords, which were protected with a cryptographic hash function that left them scrambled but less effectively than full encryption would have. And there even were firewalls for the PlayStation Network, but a former Sony engineer told the plaintiffs they were installed "on an ad-hoc basis" after the company "determined that a particular

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

user was attempting to gain unauthorized access."[7] Whether these protections constituted "reasonable, adequate and industry-standard security measures" was open to debate, in large part because there was no clear, codified industry standard for cybersecurity. Undoubtedly, Sony had made some missteps and could have provided stronger security to its customers but, at the same time, the plaintiffs' allegations that the company failed to update software, encrypt data, or use firewalls were not entirely accurate, either.

In a further attempt to show that Sony knew its protections for customer data were inadequate, the plaintiffs pointed out that the company had invested significantly more resources in protecting its own proprietary intellectual property and data with "firewalls, a debug unit and IP address limitations." These stronger security measures on another part of the company's networks made the relatively weaker security for customer data all the more egregious in the eyes of the breach victims. "While Sony knew that these basic security measures were necessary to protect its proprietary systems, it chose to cut corners when it came to its customers' Personal Information and failed to implement similar safeguards" for the PlayStation Network that stored customer data, the complaint alleged. But here, again, it was not clear whether Sony's stronger security for proprietary company data was an indication of its negligence in protecting customer data less rigorously or merely a routine—even sensible—decision to prioritize protection of the company's highest-value assets.

Similarly, the plaintiffs' contention that Sony should have been aware that a security breach was imminent was tenuous. Earlier in 2011 Sony had sued a nineteen-year-old named George Hotz who had figured out how to modify PlayStation consoles so they could be used to play games that were not manufactured by Sony. The copyright infringement lawsuit that Sony filed against Hotz was controversial and it had attracted attention from hacker group Anonymous which, two weeks prior to the 2011 PlayStation breach, sent Sony an ominous message: "You have abused the judicial system in an attempt to censor information on how your products work. . . . Now you will experience the wrath of Anonymous. You saw a hornet's nest and stuck your penises in it. You must face the consequences of your actions, Anonymous style. . . . Expect us." The class action complaint stated, "Despite this direct threat to imminently breach the Network, Sony unreasonably and unfairly failed to implement adequate safeguards to protect its Network, including failing to

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

take steps to protect Plaintiffs' and the other Class members' Personal Information stored on its Network."[8] But it's difficult to see what, exactly, Sony should have known or been expected to do upon receiving such a threat.

In its response to the complaint, Sony dismissed the plaintiffs' claim of negligence as "wholly conclusory," writing that "pointing by hindsight to the fact that an intrusion occurred does not establish, or permit an inference, that security was not reasonable. Nor does parroting unidentified commentary from blogs about firewalls make it plausible that a firewall was somehow involved in the intrusion." To fight the class action lawsuit, Sony had to take the stance that it had had reasonable security protections in place and had not been negligent in its security—that the harm to the individual victims had come from the perpetrators. To fight the later denial of coverage by its CGL insurers, however, Sony would have to make exactly the opposite case. But in 2012, Sony's priority was trying to get the class action lawsuit dismissed rather than rounding up insurance coverage for the associated costs. So, in keeping with a pattern that had been relatively successful in other breach lawsuits, Sony motioned for the class action suit to be dismissed on the grounds that none of the plaintiffs alleged "any actual harm from exposure of his or her accountholder information." To support its motion, Sony pointed out that "numerous courts have held that allegations of mere exposure of a plaintiff's personal information . . . are insufficient to state a claim for negligence."[9] Despite Sony's best efforts, in an October 2012 ruling, Judge Battaglia allowed the class action complaint to move forward, ruling that the loss of the PlayStation customers' personal data was sufficient injury to grant them standing to sue Sony.

ZURICH V. SONY: PANDORA'S BOX

On February 21, 2014, five months before the $15 million Sony class action settlement agreement was reached, lawyers for Sony and Zurich, as well as several of Sony's other insurers, squared off in a courtroom in Manhattan before Justice Jeffrey K. Oing. The two sides disagreed about whether the CGL policies that Sony had purchased from Zurich and other insurers covered any of the costs incurred by the breach—most notably the mounting legal fees. Sony's CGL insurance included coverage for "personal and advertising injury," which was defined broadly in the policy itself as:

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

injury including consequential bodily injury arising out of one or more of the following offenses . . .

(A) false arrest, detention or imprisonment.
(B) malicious prosecution.
(C) the wrongful eviction from wrongful injury into or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies committed by or on behalf of its owner, landlord or lessor.
(D) oral or written publication in any manner of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services.
(E) oral or written publication in any manner of the material that violates a person's right of privacy.
(F) the use of another's advertising idea in your advertisement.
(G) infringing upon another's copyright, trade, dress or slogan in your advertisement.[10]

The fight in the New York courtroom hinged on paragraph (E) of that definition, specifically on whether or not the breach of seventy-seven million Sony PlayStation customers' personal data counted as the "oral or written publication in any manner of the material that violates a person's right of privacy." Zurich's lawyer Kevin Coughlin and Mitsui's lawyer Robert Marshall argued that it didn't because the stolen data had not been "published" and because, even if it had, Sony had not performed that publication itself—rather, outside hackers had. On the other side, Richard DeNatale, a lawyer representing Sony, insisted that the CGL policy was intended to cover "a wide variety of privacy torts" and pointed out to the judge that the relevant clause in paragraph (E) had "no limitations or restrictions that depend upon who makes the disclosure, how the material is disclosed or to how many people the material is disclosed."[11]

Coughlin emphasized that "the Zurich policy as well as the Mitsui policy was never intended to cover cyber losses," highlighting the extent to which insurers regarded these costs as a separate category and one they were eager to exclude from their existing policies. Coughlin's language also made clear that he was arguing for an exclusion of not just data breach–related claims and liability but, more broadly, a whole class of "cyber losses" that Zurich did not intend their policies to cover when they wrote them. But the crucial question for resolving what the CGL policy did or did not cover did

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

not lie in its authors' intentions but rather in the language of the policy itself. Indeed, in court, Justice Oing dismissed Coughlin's point, responding that "whatever your intent is, the bottom line is that I'm restricted to what the policy terms are."

Aside from the insurers' intent, there was also much disagreement in the courtroom about whether what had happened in the Sony case actually constituted a "publication." Coughlin argued that, in the case of the breach, "there is a total absence of publication." Indeed, while Sony had confirmed that their customers' data had been stolen, that data had not been publicly posted or published anywhere (in fact, the allegations of harm raised in the class action lawsuit focused primarily on the possibility that the data might be sold in underground online forums at some future date). Marshall insisted that "the plaintiffs are only alleging that they have a fear that the hackers may [publish the stolen information]. But, there is no allegation that the hackers themselves published anything."

DeNatale countered these arguments by invoking several previous cases that deemed "situations of passive access to information or inadvertent access to information" to be instances of publication. For instance, he cited a West Virginia case in which a hotel installed surveillance cameras that could be viewed from the manager's office and a court later found that "the fact that there were people who could inadvertently see those clients and see the recordings . . . was a publication." He also referenced a case in which baby monitors installed in confidential counseling sessions in Oklahoma were held to constitute a publication, and another in which a LensCrafters glasses store in California allowed someone to sit in on customer's eye exams and had access to customers' confidential information in a manner that was later deemed a "publication" by a court. Marshall countered with his own, loosely related precedent, citing a case in which someone hacked into a company called Prodigy Services, created a fake email account and then sent obscene emails from that account and the recipient sued the company. In that case, a New York court found that the security breach did not involve a "publication" but, as Oing pointed out, it was not a perfect parallel to the Sony breach. "That's hacking into a system to send a message," Oing told Marshall. "This is different. This is hacking into a system and getting information out."

For his part, the judge seemed sympathetic to the view that a potential future publication by the hackers could constitute a publication in line with the particulars of Sony's CGL coverage. "I look at it as a Pandora's box," Oing

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

said in court. "Once it is opened it doesn't matter who does what with it. It is out there. . . . And whether or not it's actually used later on to get any benefit by the hackers, that in my mind is not the issue. The issue is that it was in their vault." However, where Oing did side with the insurers, ultimately, was in ruling that the CGL policy covered only acts of publication performed by Sony itself rather than by third parties like hackers. "This would have been a totally different case if Sony negligently opened the box and let all of that information out," he said. "This is a case where Sony tried or continued to maintain security for this information. It was to no avail. Hackers got in, criminally got in. They opened it up and they took the information. . . . I am not convinced that that is oral or written publication in any manner done by Sony. That is an oral or written publication that was perpetrated by the hackers."

While Sony tried to convince the court that the inclusion of the words "in any manner" in the phrase "oral or written publication in any manner" in their CGL coverage implied that it covered all forms of publication, including those by third parties, Oing took that to mean that the coverage applied only to publication through any medium (e.g., fax or email) not by any party. Even though that particular clause of the CGL policy did not specifically state that the policyholder had to be the one to publish the information, the rest of the policy strongly suggested that was the case, Oing found. "This entire policy . . . it's very policyholder oriented," Oing pointed out. He continued:

> Everything talks about the policyholder has to do this, the insured has to do that; this, that. Now, we get down to this one area here where you are saying, no, that does not mean insured only. It means anybody. So that you're asking me in that sense now to carve-out this little island for you. . . . When you point to E you say that has to be treated differently, like the tail wagging the dog. . . . E can only be in my mind read that it requires the policyholder to perpetrate or commit the act. It does not expand. It cannot be expanded to include 3rd party acts. As we are going back and forth, back and forth, the policy could be read this way and that way, the bottom line is it is written the way it is written.

The crux of Oing's ruling in favor of Zurich and Sony's other CGL insurance providers was that CGL policies only applied to damages policyholders were legally obligated to pay due to affirmative measures they had taken rather than intrusions or liability caused by third parties (in this case, the hackers). In the cases of the hotel installing surveillance cameras or LensCrafters allowing someone to be present at eye exams, the company in question had made a

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

conscious decision to violate their customers' privacy, or as Marshall put it in court, "every case cited by Sony in support of the proposition that negligent security can be equated with publication, again, involved affirmative conduct by the insured." To the insurers—and Oing—these examples of "affirmative conduct" were quite unlike the PlayStation breach where Sony was at fault for providing negligent security only insofar as it had failed to make conscious decisions to better protect its customers' data.

That failure to protect data, or rather, Sony's decision to provide its customers with negligent security, was what Sony was counting on to justify its use of CGL coverage. In fact, when Oing pressed DeNatale on the question of whether he really believed that CGL policies could cover the acts of third parties, DeNatale acknowledged that the coverage was for actions committed by the insured party. "But, it covers you for acts of negligence," DeNatale added. "CGL policies traditionally cover you for acts of negligence. If someone falls on your premises you haven't pushed them over." In other words, Sony's argument hinged on the idea that they were very much at fault for the breach because they had been negligent in failing to protect their customers' data—in much the same way that a company might be negligent for failing to shovel the snow off the sidewalk in front of their premises and causing someone to fall. Across the country in California, the class action lawsuit that Sony was fighting at the same time against its own customers affected by the breach required them to make exactly the opposite argument: that they had not been at all negligent in their data security practices, merely the unlucky, unsuspecting victims of sophisticated adversaries and were therefore not liable for the harm that had befallen their customers.

Coughlin pointed out the hypocrisy of Sony trying to make both of these arguments simultaneously in parallel court cases. He told the court, "they were arguing in the consolidated class action that we didn't do anything wrong. We didn't disclose anything. We didn't publish anything. We did nothing. We are a victim." And, indeed, that argument that Sony was pushing in the class action case was the interpretation of the breach that Oing seemed to most agree with, telling Sony:

> the totality is . . . that your security features weren't sufficient to prevent hackers from coming in and getting access. While the plaintiffs have to say that you guys breached the duty to them, I mean, they are not going to sue the hackers because they cannot find the hackers. They can find the guy that had all of the information. That's you. . . . So, Sony is the victim here.

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

It's a view that would have been most welcome to Sony had it come from Battaglia, the judge presiding over the consolidated class action complaint filed by Sony's customers—that Sony was the victim, and its customers were only suing because they didn't know who the responsible hackers were and therefore couldn't sue them. In that case, however, Battaglia had been willing to let the class action suit move forward, otherwise Sony would probably not have needed to try to exercise its CGL coverage in the first place.

The striking parallels and contradictions between the two cases tied to the Sony breach playing out simultaneously on opposite coasts speak to the challenges that both Sony and its customers faced in trying to navigate the unclear liability regimes governing cybersecurity incidents in the early 2000s. In one case, Sony was exploring the limits of the personal and advertising injury coverage in its CGL insurance in light of a relatively new type of threat and in the other it was exploring the limits of its responsibility for protecting its customers from that same threat. Oing told the court in 2014:

> in this case it is without doubt in my mind, my finding is the hackers did this. The 3rd party hackers took it. They breached the security. They have gotten through all of the security levels and they were able to get access to this. That is not the same as saying Sony did this.

But later considerations of liability for cybersecurity breaches would complicate that clear-cut distinction between cases where the attackers were responsible and ones where the defenders were at least partly to blame.[12]

The liability considerations around security breach class action suits would become more complicated over time, as courts developed more nuanced interpretations of how the loss of personal information could harm people and regulators around the world developed more stringent sets of digital privacy rights. But the precedent set by Oing's ruling on the applicability of CGL policies to data breaches and other types of "cyber losses" would remain straightforward and highly influential. In the years following Oing's ruling, other companies that tried to exercise their CGL coverage in the face of cybersecurity incidents found that it was often no help at all. The confusion, uncertainty, and technical issues surrounding data breach liability echo some of the reasons insurance reformers proposed the no-fault model for auto liability insurance, in recognition of the fact that "in motor vehicle accident cases, the principle of negligence is peculiarly difficult to apply."[13] While breaches may not occur

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

with the same frequency or suddenness as car accidents, it is also often difficult to reproduce exactly the chain of events that led up to an incident, given the challenges of digital forensic investigation, and juries and judges are often ill-equipped to understand many of the technical details that arise in the course of these investigations. The argument that auto liability litigation "results in jury trials which are largely contests of skill and chance," as the Columbia report put it, could equally well be applied to many of the data breach liability suits, and there is a significant burden on victims to pursue these suits and justify the injuries they have suffered, though that burden is distributed much more widely since data breaches typically involve far more victims than car accidents. If it were possible to more clearly delineate a set of baseline cybersecurity measures and practices for firms, it's conceivable that some principles of no-fault insurance might be applicable to breach liability insurance as a means of compensating victims quickly and reducing the amount of energy and effort expended on deciding who is at fault in these circumstances where, so often, many different parties are deserving of some degree of blame.

INNOVAK INTERNATIONAL INC. AND INDIRECT PUBLICATION

The 2014 ruling in *Zurich American Insurance Co. v. Sony Corp. of America et al.* set the stage for other insurers to fight their customers' attempts to use CGL and other non-cyber-specific policies to cover online intrusions and security breaches. For instance, in 2016, in a very similar dispute, accounting and payroll services provider Innovak International Inc. turned to its CGL policy provider, the Hanover Insurance Company, when it faced a data breach class action lawsuit. The class action complaint, filed in Alabama, alleged that Innovak had been aware of software vulnerabilities in its systems since 2014 and had failed to patch them, enabling the subsequent breach. Furthermore, the plaintiffs alleged, they had learned about the breach of their personal data not from Innovak but instead from the IRS, which sent letters informing them that their social security numbers, birthdates, addresses, and telephone numbers had been compromised. The loss of their personal information had caused "psychic injuries," the plaintiffs alleged, and some of them also said that their stolen information had been used to file fraudulent tax returns. As a result of those emotional and financial losses, caused by Innovak's negligent security, the plaintiffs demanded that Innovak pay compensatory and punitive damages, as well as

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

attorney's fees.[14] Innovak moved swiftly to dismiss the suit, but that motion was denied on August 4, 2016, by district judge W. Keith Watkins.[15]

It wasn't the outcome Innovak was hoping for, but the company had already begun to prepare for the possibility that the class action litigation might move forward. On July 19, 2016, a few weeks before Watkins issued his order allowing the class action suit against Innovak to move forward, Innovak had filed its own lawsuit in Florida against Hanover. Innovak was seeking a declaration from the Florida court that Hanover was "contractually obligated" to cover the breached payroll company's legal fees in the class action suit in Alabama under the CGL policy it had sold to Innovak.[16]

Because CGL policies are so standardized across the industry, Innovak's CGL policy from Hanover was very similar to the one Sony held with Zurich and covered liability losses resulting from personal and advertising injuries in almost exactly the same terms as the Sony policy, including injuries arising out of "oral or written publication, in any manner, of material that violates a person's right of privacy."[17] But there was one notable difference between the two CGL policies—a difference that suggested Innovak might have more luck fighting Hanover in court than Sony had had with Zurich and its many other insurers. Two years after the Sony decision—perhaps even in part because of it—Innovak also had specific provisions for data breaches in its CGL policy. The Data Breach Form portion of Innovak's CGL policy with Hanover stated:

> We will provide Data Breach Services, Data Breach Expense Coverages and Additional Expense Coverages . . . if you have a "data breach" that:
>
> a. Is discovered during the coverage period of this Data Breach Coverage Form; and
> b. Is reported to us within 30 days of your discovery of the "data breach."

However, the Data Breach Form also explicitly noted that it would not cover "any fees, costs, settlements, judgments or liability of any kind arising in the course of, or as a result of a claim for damages, lawsuit, administrative proceedings, or governmental investigation against or involving you." Instead, the Data Breach Form—rather peculiarly for a CGL policy—seemed to focus exclusively on first-party breach costs, such as notification, public relations consulting, or forensic investigation.

On June 13, 2016, at the start of the class action lawsuit and one month before Innovak went to court to try to compel its insurer's support in the

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

class action suit, Hanover issued a denial of coverage letter to Innovak that echoed the arguments Zurich had made so successfully against Sony. "Here, third party hackers, not the Insured, caused the data breach," Hanover pointed out. The carrier also ruled out coverage under the Data Breach Form because that section of the CGL policy explicitly excluded coverage for costs related to legal services or liability litigation and also noted that Innovak had failed to notify them of the breach within the thirty-day period required by the Data Breach Form.

In court, Innovak conceded that it would not try to claim coverage under the bodily injury or property damage provisions, or even the Data Breach Form, but, like Sony, the company argued that the circumstances of its breach qualified as a "publication" that violated its customers' right of privacy. Bolstered by Zurich's success in 2014, Hanover essentially repeated all of the same arguments that Sony's insurers had made in court two years prior. Hanover argued first that there had been no publication of the stolen data, only "appropriation" of the information "by third party hackers," and then argued that even if the court did consider the stolen data to have been published, that publication was done by a third party, not Innovak. Finally, Hanover's lawyers said, even if Innovak was found to have, in some sense, "published" the stolen data through its negligence, the CGL policy *still* would not apply because it covered only "intentional acts by the insured," and Innovak's failure to implement strong data security could hardly be viewed as an intentional act.

Innovak, understandably, mimicked Sony's arguments less closely, choosing a new precedent on which to base its argument. Innovak focused on a 2013 California case between Hartford Casualty Insurance Company and one of its customers, a business called Corcino & Associates, that had provided a job applicant with some confidential medical information supplied by Stanford Hospital and Clinics and asked the applicant to "perform certain tasks with the data" as part of her application, including converting the spreadsheet into bar graphs and other charts. The applicant, apparently unable to complete those tasks, turned to the Internet for assistance, posting the data and associated tasks on a website called "Student of Fortune," where students asked for help with homework and assignments. The data that the job applicant posted, along with the request for help, included the names of nearly 20,000 patients of Stanford Hospital's Emergency Department as well as their medical records, diagnosis codes, dates of their admission

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

to and discharge from the hospital, and billing charges. The patients whose information was revealed later sued, and Corcino turned to Hartford Casualty Insurance Company, the provider of its CGL coverage, for support in the suit. Hartford filed a suit claiming the breach was excluded from its CGL coverage but Judge Gary Allen Feess dismissed the suit on October 7, 2013.[18]

Though Feess's decision hinged on whether or not the privacy violation for the affected patients derived only from statutory privacy protections, Innovak attempted to repurpose the ruling to show that third-party leaks of information could trigger CGL coverage. If the job applicant's actions were covered under Corcino's CGL policy, then why shouldn't the actions of the hackers who breached Innovak's online portal also be covered? Judge Mary S. Scriven, who presided over the Innovak decision, was unimpressed by this logic. "Corcino is wholly inapposite," she wrote in her November 17, 2017, ruling rejecting Innovak's attempts to force Hanover to provide coverage. Scriven continued:

> Notably, Corcino involved allegations that private information was actually posted by the insured, through one of the insured's job applicants, to a public website, which connotes a "publication" of information. Here, the Underlying Claimants [who filed the class action suit against Innovak] do not allege that their [personal private information] was ever made publicly accessible by Innovak.[19]

Scriven's assertion that Corcino "actually posted" the private information is striking since, in fact, Corcino did not post the information; an applicant for one of its positions did. Unlike an employee of Corcino, the job applicant could hardly be seen as acting as a legal agent of Corcino when she posted the confidential data in an attempt to get help with her application. However, Corcino did deliberately turn over the data to that applicant, unlike Innovak, which did not intentionally provide its customers' data to the hackers who stole it. If it had, perhaps it would have been in a better position to exercise its CGL coverage—a somewhat confusing conclusion from a cybersecurity perspective since turning over the data would, to some extent, imply even laxer security than a series of failed defenses.

Corcino could perhaps have been said to have indirectly published the information from Stanford Hospital's Emergency Department, a line of reasoning that Innovak also tried to invoke in court, arguing that it had, in some sense, indirectly published the stolen information by failing to protect it. But Scriven was also unwilling to entertain that notion, primarily

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

because the class action complaint brought against Innovak did "not contain any allegations of indirect publication by Innovak." She said of the class action lawsuit, for which Innovak was seeking coverage, that the plaintiffs "repeatedly contend that Innovak failed to protect their [personal private information] by failing to implement sufficient data security measures" and concluded that this "is not an allegation of indirect publication; it is not an allegation of publication at all."[20] In this regard, Scriven seemed to take an even sterner line than Oing in interpreting the constraints of a CGL policy's relevance to data breaches, contending that the parties affected by the breach must themselves allege publication—or indirect publication—in order for the breached firm to invoke its CGL coverage. In the Sony suit, by contrast, Oing appeared relatively unconvinced by the argument that a data breach was not a form of publication. He indicated that he viewed a breach as tantamount to publication in many ways with his reference to Pandora's box and statement that "Once it is opened it doesn't matter who does what with [the stolen data]. It is out there."[21]

The discrepancy between Oing's and Scriven's perspectives on what constitutes publication in the context of a data breach is important because many—if not all—of the risks associated with breaches stem from the possibility that the stolen data will be made available to parties who will be able to use it for harmful or malicious purposes, ranging from financial fraud and identity theft to extortion and espionage. Scriven's ready dismissal of the possibility that a data breach could be considered a form of publication, or even indirect publication, suggests a relatively narrow interpretation of the term "publication" as meaning "public dissemination" and a short-term view of the consequences of a data breach. This interpretation of what it means to publish data would render CGL policies inapplicable to most breaches, with the possible exception of those that explicitly aim to publish stolen data in as public a manner as possible, like the 2014 Sony Pictures breach.

Despite their divergence on the question of whether a data breach can function as a form of publication, and how that question should be answered, there is no doubt that Scriven's ruling was heavily influenced by Oing's earlier one. Scriven noted that "case law on the subject is scant," but referenced the Sony case as the one instance in which a "court has addressed this issue in the data breach context." Scriven cited Oing's decision that the CGL policyholder must "perpetrate or commit the act" of publication and that, in the case of a breach, that publication is perpetrated by the

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

hackers. "The Court concurs in that reasoning and finds that the only plausible interpretation . . . is that [Innovak's policy] requires the insured to be the publisher," Scriven wrote. Scriven's ready dismissal of the arguments that Innovak's CGL policy might apply to a data breach class action lawsuit speaks to how influential Oing's ruling was already in 2016 as the only case that had dealt with the question of whether CGL insurance covered breach lawsuits. Scriven suggested, in declining to equate a data breach with an act of publication, that she might be willing to go even further than Oing in blocking data breaches from being considered covered forms of personal or advertising injuries. Oing's reasoning, therefore, acted in some sense as a moderating influence in the Innovak decision, allowing Scriven to stop short of the most extreme opinions she hints at in her ruling about the inapplicability of CGL coverage to data breaches.

ROSEN HOTELS & RESORTS AND COVERAGE FOR BREACH NOTIFICATION COSTS

Both the Sony and Innovak disputes with the carriers of their CGL policies involved pending class action lawsuits brought by their customers, who were attempting to hold the companies liable for the loss of their data. Those suits and the looming liability they posed made CGL policies in some sense the obvious focus of the breached companies, but CGL claims regarding data breaches were not limited to incidents that led to class action lawsuits. In at least one case, a CGL insurance carrier took steps to avoid covering breach costs even in advance of any such lawsuit being filed—emboldened no doubt by the success of Zurich and Hanover in fighting off breach-related claims. On February 3, 2016, Florida hotel chain Rosen Hotels & Resorts Inc. received the first reports from payment card networks that a pattern of fraudulent activity had been tied to customers of its hotels. Rosen paid an independent firm $150,000 to examine its systems and the investigation revealed several periods of long-lasting breaches of the hotel chain's payment card information beginning in September 2014 and continuing all the way through February 2016.

Following this investigation, on March 4, 2016, Rosen notified the affected customers of the breach. The notification process cost Rosen more than $100,000, with $50,000 going to pay the company's lawyers, another $15,000 to a crisis management firm, and a final $40,000 in costs for issuing the

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

notifications themselves. But those costs were trivial compared to the fines that Visa, MasterCard, and American Express levied against Rosen upon learning of the breach. Rosen had signed card service agreements with each of the major payment networks to process payment cards belonging to the networks, and all three networks determined that Rosen, in failing to protect its customers' data, had been in violation of those agreements and had caused major payment fraud losses to the payment networks and issuing banks responsible for covering fraudulent charges. MasterCard and Visa each issued fines of more than $1 million to Rosen, and American Express fined the company an additional $128,830 in connection with the breach.[22]

On December 29, 2016, at the end of a tumultuous (and expensive) year, Rosen Millennium, a wholly owned subsidiary of Rosen Hotels & Resorts that provided data security services for the hotel chain, sent a brief Notice of Claim letter to its insurer, St. Paul Fire & Marine Insurance Company: "Credit card systems breach. Loss dates range from Sept 2014 thru Feb 2016." Rosen's insurance broker later informed St. Paul that Rosen would be seeking coverage for damages resulting from the breach under its CGL policy with St. Paul. On March 2, 2017, St. Paul issued a coverage denial letter stating that it would provide no coverage for the breach under Rosen's CGL policy, but allowing that Rosen might provide additional information that could influence that determination. Later that month, on March 24, 2017, St. Paul sued Rosen in Orlando, Florida, asking the court to make a declaratory judgment that the CGL policy St. Paul had sold to Rosen did not cover any of the damages associated with the data breach.[23] More than a year later, on June 8, 2018, with the suit still pending in court, Rosen sent a letter to St. Paul demanding payment for the breach costs.

The standard-form CGL policy Rosen had purchased from St. Paul had limits of up to $1 million per event, $1 million for advertising injury per person, and $1 million for personal injury per person, as well as an overall $2 million aggregate limit. Since Rosen's costs for the breach totaled roughly $2.4 million, according to St. Paul's complaint, the policy could potentially have covered a significant portion of those losses had Rosen been able to classify them as resulting from personal or advertising injuries. The personal and advertising injury offenses specified in the policy included "Making known to any person or organization covered material that violates a person's right of privacy." The policy included no definition of what it means to make material known, but both parties later agreed the

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

requirement was synonymous with "publication," though, as in the Sony and Innovak cases, they disagreed on whether the breach involved any such publication of the stolen data.[24]

St. Paul relied heavily on the logic of the 2014 Sony ruling and 2016 Innovak ruling to make the case that Rosen itself would have had to make the stolen credit card information known in a manner that violated its customers' privacy in order for the policy to provide coverage. Rosen, in turn, couched itself as responsible for the breach in its demand letter, writing that it had "made private information known to third parties that violated a credit card holder's right of privacy."[25] This language both mirrored the personal injury definition in the CGL policy and also framed Rosen as the perpetrator of the breach. The penalties issued by Visa, MasterCard, and American Express, which comprised the bulk of the costs Rosen faced, St. Paul also regarded as falling outside the covered classes of injury. Those fines were further excluded from coverage, in St. Paul's view, because of a clause in the CGL policy stipulating, "We won't cover injury or damage for which the protected person has assumed liability under any contract or agreement."[26] Rosen disagreed, claiming that the personal injury provisions of its CGL policies applied to the breach notification costs, and also arguing that the need to replace stolen credit cards—for which the payment networks fined Rosen—should be covered as "property damage" under the policy.[27]

In keeping with the Sony and Innovak rulings, the deciding district judge in the Rosen dispute, Carlos E. Mendoza, concluded that St. Paul was not liable for any of Rosen's breach-related costs because the "alleged injuries did not result from Millennium's business activities but rather the actions of third parties."[28] Rosen, like Sony and Innovak before it, attempted to find relevant precedent in earlier insurance cases unrelated to data breaches, invoking one case in which a company accidentally posted patient records online, and another in which a firm published a customer's DNA test results on its website without consent. In both of those cases, courts had ruled that the insurers had a duty to defend the companies in questions under CGL policies—but, as Mendoza pointed out, neither one involved disclosure by a third party. They also involved more unambiguous examples of "publication" than the Rosen case did.

Perhaps hoping to squash any debate over whether its breach could be considered an act of publication, Rosen invoked a more surprising case, involving spyware. The spyware insurance dispute stemmed from a couple

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

named Crystal and Brian Byrd who, in July 2010, leased a laptop from a store called Aspen Way. On December 22, 2010, a manager from the store showed up at their home to reclaim the computer because he believed, incorrectly, that the Byrds had fallen behind on their lease payments. The manager showed the couple a picture of Brian Byrd at the computer that had been taken with the laptop's camera. The Byrds later learned the photo been taken using a program called PC Rental Agent that can capture a computer's keystrokes, take photos with its camera, and take screen shots. The Byrds then filed a class action suit against Aspen Way in May 2011 alleging that the retailer had violated the Electronic Communications Privacy Act by intentionally disclosing private data to a store employee. The State of Washington also sued the company on similar charges in October 2013, and Aspen Way turned to its insurance provider, Liberty Mutual, to provide coverage for its legal defense in both suits.[29]

Liberty Mutual and Aspen Way's other insurers were ultimately able to get out of covering the retailer's legal defense costs thanks to an exclusion in the policy that explicitly ruled out coverage for "recording and distribution of material or information in violation of law." While that exception did not apply to Rosen's situation, the *Aspen Way* ruling was relevant in another regard to their case because it dealt directly with the question of the circumstances under which data could be considered "published" and did so in a fashion much more charitable to breached entities than the *Innovak* or even *Sony* rulings. In the Aspen Way dispute, Montana district judge Susan P. Watters determined that the meaning of "publication" included "the dissemination of information to at least a third party, if not the public-at-large." Watters explained: "This liberal definition of 'publication' conforms with Montana's strong policy of construing insurance policy terms in the insured's favor."[30] This very generous interpretation of publication—as disclosure to even just one third party—stood in contrast to the narrower definition Scriven had seemed to espouse in the Innovak case and hinted at a possible path for construing a data breach as a privacy injury.

But ultimately, Mendoza—like Oing and Scriven before him—determined that because third-party hackers had infiltrated Rosen's networks and violated its customers' privacy, rather than the hotel chain accidentally publishing its customers' information itself, Rosen's CGL policy did not apply to the incident, regardless of whether or not an act of publication had taken place. The precedent set by the Sony, Innovak, and Rosen cases regarding large-scale

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

data breaches and the resulting massive class action lawsuits speaks to how effective insurers were at explicitly carving out coverage for that type of liability from CGL policies. The privacy injuries described in these policies were so narrowly defined that the definitions applied to only a very narrow set of incidents in which a company publishes customer information itself and thereby excluded all data breaches perpetrated by outside hackers. Those rulings were a victory for insurers on two levels. First, they allowed insurers to avoid paying the legal costs for a string of these class action lawsuits. But perhaps even more importantly, the rulings sent a strong message to businesses concerned about the growing risk of data breaches: if they wanted any protection for such incidents, then they would have to buy an entirely new type of insurance. Underlying that definitive exemption of data breaches from CGL coverage, however, was a much more complicated and unresolved set of liability issues that the insurance disputes barely touched on beyond forcing breached companies like Sony to argue both of their conflicting roles as breach victim and enabler at once, in parallel lawsuits. The CGL disputes over coverage for breach liability laid bare the contradictions and inherent challenges of trying to untangle who was responsible for incidents that had multiple, often overlapping, layers of victims, enablers, and potential defenders.

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a portion of the eBook at doi:10.7551/mitpress/13665.001.0001

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

This is a section of doi:10.7551/mitpress/13665.001.0001

Cyberinsurance Policy

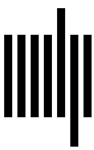
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

By: Josephine Wolff

Citation:

Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks
By: Josephine Wolff
DOI: 10.7551/mitpress/13665.001.0001
ISBN (electronic): 9780262370752
Publisher: The MIT Press
Published: 2022

The open access edition of this book was made possible by generous funding and support from MIT Press Direct to Open



The MIT Press

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025

MIT Press Direct

© 2022 Massachusetts Institute of Technology

This work is subject to a Creative Commons CC-BY-NC-ND license.
Subject to such license, all rights are reserved.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Bembo by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data

Names: Wolff, Josephine, author.
Title: Cyberinsurance policy : rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks / Josephine Wolff.
Description: Cambridge, Massachusetts : The MIT Press, [2022] | Series: Information policy series | Includes bibliographical references and index.
Identifiers: LCCN 2021045988 | ISBN 9780262544184 (paperback)
Subjects: LCSH: Computer insurance. | Computer security—Management. | Cyberspace—Security measures—Management. | Computer crimes—Prevention. | Risk management.
Classification: LCC HG9963.5 .W65 2022 | DDC 658.4/78—dc23/eng/20220114
LC record available at https://lccn.loc.gov/2021045988

Downloaded from http://direct.mit.edu/books/oa-monograph/chapter-pdf/2239813/c001500_9780262370752.pdf by guest on 13 February 2025