PROGRAM MATERIALS
Program #29179
November 11, 2019

Will Your Cyber Policy Pay for the Inevitable Breaches?

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

PERKINSCOIE

COUNSEL TO GREAT COMPANIES

West/Thomson Reuters CLE Webcast

WILL YOUR CYBER POLICY PAY FOR THE INEVITABLE BREACHES?

November 11, 2019

Norton Cutler
Bradley Dlatt

COUNSEL TO GREAT COMPANIES

Need for Cyber Liability Coverage

The Rise of Data Breaches

- Over 3,800 data breaches reported during the first six months of 2019
- More than 54% increase over each of the past four years
- Chance of a business having a breach in next 2 years = **30%**

Sources: Risk Based Security, 2019 MidYear QuickView Data Breach Report (Aug. 2019); https://helpmewithhipaa.com/cost-of-a-data-breach-2019-study-ep-217/

The Rise of Data Breaches

Major Cost Decrease Factors (Mitigators) Included:

- Forming an Incident Response Team
- Extensive Test of Incident Response Plan
- Business Continuity Management
- Employee Training
- No matter what precautions you take, a regulator or a class action lawyer will blame you for the breach and seek damages

Understanding the Increased Risks to Your Business

Types of Information That Hackers Target:

- Financial data
- Personal information of your employees or customers
- Sensitive business information (trade secrets)
- Health information
- Internal communications portals
- User accounts

Understanding the Increased Risks to Your Business

- Average reported cost of responding to a data breach for an American Company: **$8.2 million**
- Cost Centers:
  - Detection and Escalation
  - Notification
  - Lost Business—largest factor: 36% of total cost
  - Post-Breach Response
  - Insureds need a policy that will pay for the cost of these inevitable breaches

Source: IBM Security, Cost of a Data Breach Report (2019), https://databreachcalculator.mybluemix.net/

First Party Claims Arising from Data Breach

- Theft and Fraud
- Investigation Costs
- Cyberextortion
- Computer Data Loss and Restoration
- Business Interruption
- Property Damage
- Crisis Management/Public Relations

Third Party Claims Arising from Data Breach

- Regulatory Claims
- Credit and Fraud Monitoring
- Common Law Privacy Claims
- Statutory Privacy and Consumer Protection Claims
- D&O/Shareholder Claims

Cyber Risk/Cyberliability Insurance

- Policies are written on a “claims made” basis
  - Strict reporting requirements
- Most Cyber Risk Policies provide multiple forms of potentially applicable coverage
  - Professional Services Liability Coverage
    - Third-party claims arising out of “Wrongful Act”—*i.e.*, error or omission in the performance of professional services
    - *E.g.*, performing technology services, services leading to invasion of privacy

Cyber Risk/Cyberliability Insurance

- "Security Event" or "Privacy Event" Coverage
  - "Security Event" = failure or violation of a computer system which results in unauthorized access to or use of information, DoS attacks, or receipt/transmission of malicious code
  - "Privacy Event" = loss related to the release of confidential or protected information
  - Also covers loss related to failure to notify the appropriate individuals of such event where required by law

Cyber Risk/Cyberliability Insurance

- Network Interruption Coverage
  - Similar to business interruption—focused on lost income
  - Triggered after computer networks are compromised for a specified period of time
- Event Management Coverage—after a breach, covers:
  - Public relations/crisis management costs
  - Investigatory costs
  - Notification costs
  - Restoring, recreating, or recollecting lost data

Cyber Risk/Cyberliability Insurance

- Cyber Extortion Coverage
  - Money paid to end a security/privacy threat
- Cyberterrorism Coverage
  - Security breach or disruption combined with intention to cause harm or intimidation in an effort to further a social, ideological, religious, or political objective
- Regulatory Actions
  - Costs to defend any regulatory action or investigation by a governmental or regulatory body in the aftermath of a breach
    - The basic policy should cover these risks

Many Policies Have an Exclusion for Violation of Statutes

"Bodily injury" or "property damage" arising directly or indirectly out of any action or omission that violates or is alleged to violate:

(1) The Telephone Consumer Protection Act (TCPA), including any amendment of or addition to such law;

(2) The CAN-SPAM Act of 2003, including any amendment of or addition to such law;

(3) The Fair Credit Reporting Act (FCRA), and any amendment of or addition to such law, including the Fair and Accurate Credit Transactions Act (FACTA); or

(4) **Any federal, state, or local statute, ordinance or regulation**, other than the TCPA, CAN-SPAM Act of 2003 or FCRA and their amendments and additions, that addresses, prohibits, or **limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of material or information**.

Example Cyber Exclusion

[Coverage excluded] for **any actual or alleged violation of any federal, state, or local statute, ordinance, or regulation**, including **but not limited to**:

1. unfair competition, restraint of trade or any other violation of antitrust laws, including, but not limited to, the Sherman Act, the Clayton Act, the Robinson-Patman Act, or
2. the Telephone Consumer Protection Act, the Can-Spam Act of 2003, and the Fair Credit Reporting Act (United States)

all as amended and any rules or regulations promulgated pursuant thereto, as well as any other similar federal, state, local, or foreign law.

Why This Matters?

Most data breach lawsuits seek statutory specified damages because there is no real provable damage.

California Consumer Privacy Act

- Effective January 1, 2010
- Covers: Any for-profit company doing business in CA that collects personal information and satisfies one of the following three trigger points:
  (1) Annual gross revenues of more than $25 million;
  (2) annually buys, “sells,” or receives or shares for commercial purposes personal information of at least 50,000 consumers, households, or devices; or
  (3) derives 50% or more of annual revenue from selling CA consumers’ personal information

Why This Matters?

- Protects “consumers”—*i.e.,* natural persons that reside in California
  - Customers and employees
- Protects “Personal Information”
  - “Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”
- Introduces several limitations on use of personal information
  - Informed consent to collect personal information, including purposes for which information will be used
  - Consumer right of disclosure for information and right to know if business is selling that information (opt out)
  - Obligation to implement security procedures and practices

Why This Matters?

CCPA Contains a Private Right of Action

- Consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of business's failure to implement and maintain reasonable security procedures and practices may bring a claim.
- Damages between $100–$750 per incident, **or** actual damages, whichever is **greater**.
- May bring class action upon 30 days written notice of violation.

CCPA also allows for CA Attorney General Enforcement

Why This Matters?

Illinois Biometric Information Privacy Act

- Enacted on October 3, 2008
- Regulates collection, use, storage, and disclosure of Biometric Information and Biometric Identifiers
  - “biometric information” includes “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual”
  - “biometric identifier” includes “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry”

Why This Matters?

BIPA Obligations include:

- Developing a written policy, made available to the public, setting a retention, storage, and destruction schedule for biometric information
- Cannot “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s” biometric identifier or information without first obtaining written informed consent obtained after providing written notice of collection/storage which identifies purpose of collection/storage and length of term of collection/storage
- Cannot “sell, lease, trade, or otherwise profit” from biometric information or identifiers
- Cannot “disclose, redisclose, or otherwise disseminate” biometric information or identifiers without obtaining consent from person/customer (with exceptions)
- Biometric information and identifiers must be stored, collected, and protected from disclosure: (1) “using the reasonable standard of care within the private entity's industry; and (2) . . . in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.”

Why This Matters?

Like CCPA, BIPA contains a private right of action

- Any “aggrieved” person. No actual harm required. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186
- For each negligent violation, liquidated damages of $1,000 or actual damages, whichever is greater
- For each willful or reckless violation, liquidated damages of $5,000 or actual damages, whichever is greater
- Includes recovery of attorney fees, costs, and opportunity for “other relief”
- Many insureds want to use biometric information as the best password for customers to access data or facilities that no one needs to remember—avoids need for hard to use two factor ID or weird long passwords

Since the January 25, 2019 *Six Flags* ruling, more than 150 BIPA Class Actions have been filed in Illinois

Why This Matters?

- BIPA has increased costs of data breach or privacy events and CCPA will do the same
- Insurer's first instinct in handling a CCPA or BIPA claim will be to point to Violation of Statutes exclusion

How to Attack the Violation of Law Exclusion Defense

Focus on Favorable Legal Standards:

- Duty to Defend Policy?
  - Is there a "potential for coverage"?
  - Eight-Corners Rule
  - One of the most favorable legal standards in civil law
- Exclusions
  - Must be interpreted narrowly
  - Insurer holds the burden of proof
  - Must clearly and unambiguously exclude coverage
- Ambiguity/*contra proferentum*: All doubts resolved in favor of insured

How to Attack the Violation of Law Exclusion Defense

Are there common law claims?

- Is there enough for a common law privacy claim? If yes, there is arguably coverage despite this exclusion
- *See, e.g.*, Fed. R. Civ. P. 15(b) (parties have the right during trial to amend pleadings to conform to the evidence)

Will Your Security Software Pass Muster Under Your Cyber Policy?

Most cyber oriented policies contain an exclusion such as:

> If a system is protected by security software, you are required to maintain and, as necessary, upgrade (at your own cost) such software so that it provides a technologically credible level of security.
>
> We will not pay for any loss caused by malicious programming if, prior to the malicious programming, you:

Will Your Security Software Pass Muster Under Your Cyber Policy?

- knew of any defect or deficiency in the security software and failed to correct it;
- failed to maintain the security software in complete working order; or
- knew of any technologically credible upgrades to the security software that could have prevented the malicious programming, and failed to make them

Will Your Security Software Pass Muster Under Your Cyber Policy?

- These exclusions are designed to make sure that the insured takes reasonable precautions to prevent cyber incursions and malware attacks
- To assure some type of certainty of coverage for using certain pre-approved software, a group of carriers, brokers, and software companies have started a project called Cyber Catalyst which has certified an initial group of security software providers which seems to cover most of the major providers of security software.
  - See: https://www.marsh.com/us/services/cyber-risk/cyber-catalyst.html

Will Your Security Software Pass Muster Under Your Cyber Policy?

- This should provide an insured with some certainty that if they buy coverage from a carrier who has certified the products and also buy a certified security product and implement it correctly, then defense costs and damages from a hack or malware attack will be covered
- Cyber Catalyst also has an annual certification process so that other providers can seek certification in the future and for new products
- What happens if your client uses a security software product which is not certified?
- Compare the functionality of that Product with the certified products

Coverage for Malware Attacks

While most cyber hacks cause no real damage, malware attacks can easily cripple an insured's data systems which are often more important than physical property. Cyber policies do seem to be covering at least some of this risk with the following clause:

> Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for **cyber-threat expense**:
>
> - for a **threat** first made directly against such **insured** during the policy period; and
> - paid or incurred by the **insured** within 60 days after receipt of such **threat**
> - We will not pay that part of any **business income** loss or **extra expense** you incur to respond to extortion or other similar threat

Coverage for Malware Attacks

We will pay for the actual:

- **electronic data recovery costs**;
- **business income** loss; and
- **extra expense** you incur due to the actual impairment of your **operations** during the **period of recovery of computer service**, not to exceed the applicable Limit of Insurance for Impairment of Computer Services—Outside Attack shown in the Declarations.

Coverage for Malware Attacks

These clauses seem to cover at least the expense of restoring data. But this coverage also seems to have some gaps, such as for loss of business income during the outage and uncertainty about ransom payments.

- This insurance does not apply to loss or damage caused by or resulting from kidnap/ransom or other extortion payments surrendered to any person as a result of a threat to do:
  - bodily harm to any person; or
  - damage to the premises or other property owned by you or held by you in any capacity.
- This Kidnap/Ransom Or Extortion Loss Payment Limitation does not apply to robbery of money or securities.

And now, the security companies have raised a red flag against the simplest and cheapest way of limiting the costs associated with data hacks demanding ransom: paying the ransom demanded to turn on the computer system again.

Properly backing up data and applications to allow restoring the software from a backup is the best way to deter future attacks, but the insurance policy should pay for whatever it takes to restore the system in 24 hours even if that is a ransom payment.

COUNSEL TO GREAT COMPANIES

Questions?

PERKINSCOIE

L. Norton Cutler

- Norton Cutler, a senior counsel in the firm's Litigation practice, focuses his practice on insurance coverage, telecommunications, technology law and privacy disputes. Norton was in charge of all insurance coverage issues for NCR Corp. from 1990 to 1993 and has recently been involved in four multimillion-dollar insurance recoveries for a large financial service company, a large newspaper chain, a mining company and a retail products company. He handled all legal matters for a large wholesale mortgage company and a telecommunications consulting company. Norton defeated one of the first targeted advertising class actions on behalf of a telecom/cable company.
- Over the years, Norton has represented US WEST and its successor, Qwest, in numerous telecom regulatory and litigation matters, including the successful appeal of a $500 million rate case and numerous state regulatory proceedings which set the rules and prices for competition between incumbent telecom carriers and new competitors. Norton was involved in representing the former US WEST in claims against Time Warner arising out of Time Warner's acquisition of Turner Broadcasting Systems and in litigation surrounding the disposition and workouts of its multibillion dollar real estate portfolio. Norton has tried over 50 arbitrations involving computer and technology disputes while at NCR and US WEST.
- In addition to Norton's experience as outside counsel to numerous technology companies, he can also provide unique insight and perspective from the inside of a telecom or technology company, having served as the associate general counsel to NCR Corp and US WEST for 13 years prior to joining the firm.

Bradley H. Dlatt

- Associate in the Insurance Recovery Practice in Perkins Coie LLP's Chicago office.
- Practice focuses on providing insurance counseling to businesses and resolving insurance coverage disputes, including assisting corporate policyholders with mediation, arbitration, and litigation against their liability insurers.
- Presents regularly on insurance coverage issues. Recent presentations have included discussing the insurance implications of the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act.
- Can be contacted at bdlatt@perkinscoie.com or 312-324-8499.

YOUR VOICE

How to prepare yourself and your clients to respond to data breaches

BY JAMES M. DAVIS AND BRADLEY H. DLATT

SEPTEMBER 19, 2019, 6:30 AM CDT

Data breaches are everywhere, and they are expensive. In the first six months of 2019, there were more than 3,800 reported data breaches (https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#1299d7a2bd54)—a 54% increase from the same period last year—exposing more than 4.1 billion records. The average reported cost of a data breach for an American company is $8.2 million (https://databreachcalculator.mybluemix.net/executive-summary).

We work every day with individuals and businesses that face the real prospect of a network intrusion, a data breach or other cyber-related event that—if successful—comes with potentially staggering costs. Experts caution businesses to treat these attacks as inevitable. In addition to looking out for our clients, lawyers and law firms themselves need to be ready.

Last October, the ABA's Standing Committee on Ethics and Professional

Image from Shutterstock.com.

Responsibility issued Formal Opinion 483 (https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf): "Lawyers' Obligations After an Electronic Data Breach or Cyberattack," which acknowledged that lawyers and law firms are a target for hackers and addressed many of the key concerns lawyers and law firms must consider when responding to a breach of their own systems. The steps in this article apply equally to your own practice.

As counselors and trusted advisers, it is our job to ensure that our clients, and our own law firms, take the necessary precautions to prepare for a possible cyber-related event.

Our experience as insurance coverage counselors for individuals and businesses informs our holistic approach, based on the recognition that a data breach is not just an IT problem, a legal problem or a public relations problem—it is an organizationwide risk.

HOW TO PREPARE FOR A DATA BREACH

Step One: Understand your risks.

James M. Davis and Bradley H. Dlatt.

As a trusted adviser, you should guide your client through a detailed risk analysis, which should focus on issues such as (1) what types of data the client is collecting; (2) when and how that data is being collected; (3) where the data is being stored; (4) how the data is being used; (5) who has access to both the collected data and the other information technology systems that the client uses; (6) how data flows through the client's various systems and who touches that data along the way; (7) what procedural safeguards are in place to protect the client's systems and data; and (8) what your client's legal obligations are with respect to its collection, use and storage of the various categories of data in the event of a breach.

The final item on this list—legal obligations—is connected to the rapidly changing areas of law affecting data. States like California have begun rolling out broad-based consumer data privacy laws that touch on data collection, use and storage. Federal law protects specified categories of data, such as health information. It would benefit you and your client to have a privacy law expert at the table in this stage.

Step Two: Build the right team.

With respect to data breach preparation and response, internal delays and communication breakdowns can mean the difference between a network intrusion that is quickly recognized and quarantined or a massive data breach that never seems to end and costs millions of dollars to resolve.

An effective team includes internal stakeholders in information technology, systems management, human resources, public relations, finance and accounting, as well as appropriate members of senior leadership. Your client's team may also include outside experts such as counsel familiar with notification and disclosure obligations, a public relations firm, technical experts and security experts.

Step Three: Secure and monitor your data.

A client must think deeply about issues such as (1) IT protections surrounding the client's data collection, use and storage; (2) the client's policies and access points for its data; and (3) ways of improving the client's incident detection capabilities.

Under a holistic approach, data security measures must also include taking steps to ensure that any individuals who have access to the client's data are trained in data security best practices and understand how to recognize and respond to threats such as phishing attempts. While this step is more technical in nature, it is critical that lawyers approach these efforts with the big picture in mind and ensure that the client consults the right experts.

Step Four: Have a plan.

It is critical for clients to have a well-developed, tested, efficient breach response plan that, among other things, immediately mobilizes your client's team to triage the breach, evaluate the extent of any exposure, begin preparing any necessary legal notices and manage internal and external messaging to maintain control of the situation.

It is critical that the client keep detailed records of the plan and any necessary documents such as insurance policies, systems information and regulations that will be required to execute the plan. It is equally important that the client practice and test its plan with some regularity.

Step Five: Have the right insurance.

Insurance can be one of your client's most valuable assets in the event of a cyber-related event. Among other things, insurance may cover the cost of (1) investigating and remedying the technical causes of a data breach; (2) retaining legal counsel to respond to and defend against any investigations or demands arising out of the breach; (3) hiring public relations or crisis management firms to manage the client's external messaging and response; and (4) resolving legal claims resulting from the breach. There are many types of insurance policies that may apply to a data breach.

IN THE EVENT OF A BREACH

Step One: Execute the plan.

In the event of a data breach, you must emphasize to your client and your client's team the importance of trusting in the client's plan (which, ideally, has been well-developed and tested) and executing it at a high level.

The proper legal response to a breach can dramatically mitigate the total response costs. In the event that your client disregarded our first few proposed steps and failed to plan for a breach, you as their counsel and trusted adviser should ensure that the right technical, legal and public relations personnel are immediately mobilized to respond to the situation.

Step Two: Get your insurers involved early and keep them involved.

Insurance policies often have strict notice provisions that require a corporate or individual policyholder to provide the insurer with notice of a claim or circumstances that may lead to a claim within a specific, limited time period. In certain jurisdictions, an insured's failure to honor a sufficiently specific notice provision in its policy may bar coverage.

Because of this, even in the early stages of a data breach, when the extent of the client's exposure may be unclear, it is important to have the client get its broker and insurance coverage counsel involved immediately. Data breaches often involve acts or events that occurred over an extended period of time but were only recently discovered.

Given the complexities of coverage, a policyholder must be careful to avoid characterizing the claim in a manner that takes the claim outside of coverage. Once your client's insurers have been notified, the client should require each insurer to acknowledge its coverage obligations, and then the client should provide regular updates (as necessary) to the insurers on the status of the claim.

Step Three: Manage external response thoughtfully.

The client should be prepared to deliver any necessary notifications, both publicly and privately, and manage any external issues as they develop. It is important in these situations that the client team speak with one voice and present a unified, confident front.

James M. Davis is a partner in the insurance recovery practice in Perkins Coie's Chicago and Seattle offices. Davis has more than 20 years of experience counseling corporate and individual policyholders on insurance issues coverage disputes, including coverage for data breaches, information

privacy claims, first party property loss and claims under additional insured and vendor endorsements. He is a member of the American College of Coverage and Extracontractual Counsel.

Bradley H. Dlatt is an associate in the insurance recovery practice at Perkins Coie. Dlatt counsels corporate and individual policyholders on insurance issues and litigates insurance coverage disputes under most corporate insurance policy forms.

ABAJournal.com is accepting queries for original, thoughtful, nonpromotional articles and commentary by unpaid contributors to run in the Your Voice section. Details and submission guidelines are posted at "Your Submissions, Your Voice (http://www.abajournal.com/voice/article/your_voice_submissions)."

Give us feedback, share a story tip or update, or report an error.

PERKINSCOIE

California Consumer Privacy Act (CCPA)

CCPA Insurance Coverage Issues: Avoiding Gaps in Your Program

Starting January 1, 2020, companies doing business in California that meet certain qualifying criteria will be subject to an entirely new sphere of risk, as California's sweeping Consumer Privacy Act (the CCPA) goes into effect.

Insurance policies are some of a company's most valuable assets during times of increased risk and uncertainty. Yet, corporate policyholders often leave money on the table by failing to thoughtfully construct their insurance program to respond to the risks inherent in their business and neglecting to properly manage potential insurance claims. In recent years, data privacy and security has become a growing source of corporate risk for businesses and presenting new, evolving challenges for risk managers and insurers.

The CCPA provides extensive protections for consumers with respect to the collection, storage, use and disclosure of a broad swath of "personal information." A failure to comply with the exacting requirements of the CCPA may expose companies to an enforcement action from the California Attorney General or lawsuits from impacted California consumers. The CCPA carries substantial per-violation statutory penalties.

CCPA'S LIKELY IMPACT ON CORPORATE RISK PROFILES AND INSURANCE PROGRAMS

- Increased data breach costs and volume of data privacy litigation
- Heightened scrutiny of Directors and Officers
- Increased insurance premiums, particularly for cyber risk/liability coverage
- Increased cost of settlements and judgments

MAJOR FORMS OF INSURANCE COVERAGE THAT MAY RESPOND TO A CCPA CLAIM

Cyber Risk/Privacy Policies: Provides claims-made "first-party" coverage for losses due to destroyed/damaged data, business interruption, physical damage and/or cyber extortion and "third-party" coverage for data breach investigations and defense of privacy liability actions.

Professional Liability/E&O Policies: Claims-made coverage for wrongful conduct in connection with the delivery of "professional services."

Directors & Officers Policies: Provides claims-made coverage for liabilities incurred by directors and officers and/or claims made against a company arising out of the conduct of the company's directors and officers.

Employment Practices Liability: CCPA's definition of "consumers" may include employees, leaving open the possibility that employees may bring CCPA claims against their employer. Covers "employment practices" claims.

Commercial General Liability: Provide occurrence-based coverage for "bodily injury," "property damage," and/or "personal and advertising injury."

Crime Policies: Covers losses due to crime or dishonesty.

Property Policies: Provides coverage for property damage resulting from specific events. Typically, it also covers loss arising from interruption to a business, whether caused by damage to your property or a business partner's property

CONSIDER THE SCOPE OF THE CCPA IN NEGOTIATING YOUR POLICIES AND PREPARING FOR A POTENTIAL LOSS

A company should never accept an off-the-shelf policy. Instead, companies should seek to customize their policies to fit their risks. With respect to the CCPA, a company's policies must cover more than a data breach or theft. Policies must cover acts arising out of the ***collection***, ***use***, ***storage*** and ***disclosure*** of "personal information," a term that is defined broadly in the CCPA. Companies should carefully review this statutory definition and think deeply about how the identified forms of "information" interact with their business. Given the broad scope of the CCPA, there is a high potential for corporate exposure. To prepare for this risk, companies must build the right team, keep good insurance records, audit their policies, and have a robust process in place to promptly report insurance claims if the company is facing a CCPA-related investigation or lawsuit.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

CCPA Insurance Coverage Issues: Avoid Gaps in Your Program

By Jim Davis, Bradley Dlatt & Selena Linde on July 10, 2019

CCPA Week Webinar (FREE), July 17, 2019 1:00 p.m. PT

Insurance policies are some of a company's most valuable assets during times of increased risk and uncertainty. Yet, corporate policyholders often leave money on the table by failing to thoughtfully construct their insurance program to respond to the risks inherent in their business and neglecting to properly manage potential insurance claims. In recent years, data privacy and security has become a growing source of corporate risk for businesses and presenting new, evolving challenges for risk managers and insurers.

Starting January 1, 2020, companies doing business in California that meet certain qualifying criteria will be subject to an entirely new sphere of risk, as **California's sweeping Consumer Privacy Act (the CCPA) goes into effect**. The CCPA will apply to any for-profit entity doing business in California that collects personal information about California consumers and meets at least one of three criteria:

1. Has annual gross revenue above $25 million;
2. Annually buys, sells or, for commercial purposes, receives or shares personal information of at least 50,000 California consumers, households or devices, or
3. Derives at least 50% of its annual revenue from selling California consumers' personal information.

Moreover, if a business is subject to the CCPA, its subsidiaries and affiliates may also be covered if they share common branding, including a shared name, service mark or trademark. **For more information about the CCPA, including a diagnostic toolkit to determine whether your business may be subject to the CCPA, click here.**

The CCPA provides extensive protections for consumers with respect to the collection, storage, use and disclosure of a broad swath of “personal information.” A failure to comply with the exacting requirements of the CCPA may expose companies to an enforcement action from the California Attorney General or lawsuits from impacted California consumers. The CCPA carries substantial per-violation statutory penalties.

CCPA’s Likely Impact On Corporate Risk Profiles and Insurance Programs

- Increased data breach costs and volume of data privacy litigation
- Heightened scrutiny of Directors and Officers
- Increased insurance premiums, particularly for cyber risk/liability coverage
- Increased cost of settlements and judgments

Major Forms of Insurance Coverage That May Respond To A CCPA Claim

Cyber Risk/Privacy Policies: Provides claims-made “first-party” coverage for losses due to destroyed/damaged data, business interruption, physical damage and/or cyber extortion and “third-party” coverage for data breach investigations and defense of privacy liability actions.

Professional Liability/E&O Policies: Claims-made coverage for wrongful conduct in connection with the delivery of “professional services.”

Directors & Officers Policies: Provides claims-made coverage for liabilities incurred by directors and officers and/or claims made against a company arising out of the conduct of the company’s directors and officers.

Employment Practices Liability: CCPA’s definition of “consumers” may include employees, leaving open the possibility that employees may bring CCPA claims against their employer. Covers “employment practices” claims.

- Commercial General Liability: Provide occurrence-based coverage for “bodily injury,” “property damage,” and/or “personal and advertising injury.”
- Crime Policies: Covers losses due to crime or dishonesty. Property Policies: Provides coverage for property damage resulting from specific events. Typically also covers loss arising from interruption to a business, whether caused by damage to your property or a business partner’s property

Consider The Scope of The CCPA In Negotiating Your Policies and Preparing For A Potential Loss

A company should never accept an off-the-shelf policy. Instead, companies should seek to customize their policies to fit their risks. With respect to the CCPA, a company's policies must cover more than a data breach or theft. Policies must cover acts arising out of the collection, use, storage and disclosure of "personal information," a term that is defined broadly in the CCPA. Companies should carefully review this statutory definition and think deeply about how the identified forms of "information" interact with their business. Given the broad scope of the CCPA, there is a high potential for corporate exposure. To prepare for this risk, companies must build the right team, keep good insurance records, audit their policies, and have a robust process in place to promptly report insurance claims in the event that the company is facing a CCPA-related investigation or lawsuit.

For more information tune in to the Perkins Coie CCPA Week webinars, including CCPA Insurance Coverage Issues: Avoid Gaps in Your Program on July 17, 2019 1:00 p.m. PT.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Preparing for Data Breaches: Data Mapping, Response Team and Insurance

By Jim Davis & Bradley Dlatt on October 25, 2019

Data breaches are **up significantly in 2019**, exposing billions of confidential records and costing companies **millions of dollars** on average per breach. Security experts counsel their clients that data breaches are inevitable as even the largest, most secure systems may be breached. In spite of this environment, many tech companies are woefully unprepared to respond to a cyber intrusion, data breach, or other cyber-related event. Are you ready?

As insurance coverage lawyers, we often work with clients to confront this organization-wide challenge after a breach has occurred. The better approach, however, is to prepare in advance by understanding your risks, building a team, securing and monitoring your data, having a well developed and rehearsed response plan, and tailoring your insurance program to a possible breach. Additionally, having counsel involved throughout the preparation and response process is critical to protect privilege, minimize legal liability, and maximize insurance coverage.

Steps to Prepare for a Data Breach

Step One: Map Your Risks

Your company's ability to prevent and/or respond to a data breach depends on understanding your risks. Every company should conduct a thorough review of its own processes and systems. Mapping your risks includes determining (1) what types of data you are collecting; (2) when and how that data is being collected; (3) where the data is being stored; (4) how the data is being used; (5) who has access to both the collected data and other information technology systems; (6) how data flows through various systems and who touches what data along the way; (7) what procedural safeguards are in place to protect the systems and data; and (8) what your legal obligations are in the event of a breach with respect to the collection, use, and storage of the various categories of your data, and how can you protect legally privileged information.

Your legal obligations are rapidly changing. Acts such as the **California Consumer Privacy Act** (effective January 1, 2020) have begun rolling out broad-based consumer data privacy laws that touch on data collection, use and storage. Other states are expected to follow suit. Federal law also protects specified categories of data, such as health information. Moreover, consumer groups are urging Congress to adopt a strict national privacy standard akin to the European Union's **General Data Protection Regulation**. Even as a company operating in the tech space with a sophisticated knowledge of programming and software, it would benefit your business to have a privacy law expert at the table during this data mapping stage. Perkins Coie is home to several attorneys with extensive experience in **privacy law**.

Step Two: Assemble Your Team

Your response team should be assembled and ready in advance of a breach. Internal delays and communication breakdowns can mean the difference between a network intrusion that is quickly recognized and quarantined and a massive data breach that never seems to end and costs millions of dollars to resolve. Identify internal stakeholders in information technology, systems management, human resources, public relations, legal, finance and accounting, as well as appropriate members of senior leadership. You may also include outside experts such as counsel familiar with notification and disclosure obligations, a public relations firm, and technical and security experts.

Step Three: Develop Your Breach Plan

Using your data and risk map, and working with the team you assembled, the next step is to develop and test a breach response plan. Goals for such a plan must include rapid mobilization of your breach team to triage the breach, quick identification of the extent of any exposure, the preparation of any necessary legal notices, protection of the legal privilege of your activities and data, and management of internal and external messaging to maintain control of the situation. It is critical to keep detailed records of the plan and of any necessary documents such as insurance policies, systems information, and regulations that will be required to execute the plan. It is equally important that your company practice and test its plan with some regularity to identify and close any gaps in the plan, including common gaps such as the inability to access core team members in the event that the company email or phone system is compromised.

Step Four: Keep Your Data Secure and Monitor Breaches

Not all companies can afford state-of-the art cyber defenses, but there are many steps businesses can take to minimize the damage caused by a data breach. Companies that want to

protect their data well should think deeply about issues such as (1) IT protections surrounding data collection, use, and storage, (2) policies and access points for data, and (3) ways of improving incident detection capabilities. Data security measures must also include taking steps to ensure that any individuals who have access to your data (including members of senior management) are trained in data-security best practices and understand how to recognize and respond to threats such as phishing attempts.

Step Five: Have the Right Insurance

Your company should not overlook the importance of insurance. By mapping your data, you and your insurers should be able to tailor a program to meet your needs in the event of a cyber intrusion, data breach, or cyber-related event. Cyber liability insurance policies vary dramatically in their coverage and are often negotiable. Insurance may cover the cost of (1) investigating and remedying the technical causes of a data breach, (2) retaining legal counsel to respond to and defend against any investigations or demands arising out of the breach, (3) hiring public relations or crisis management firms to manage the client's external messaging and response, and (4) resolving legal claims resulting from the breach. You might also identify insurance coverage maintained by your business partners and vendors under which you are covered as an additional insured. Involving coverage counsel early in this process will help you get the coverage in place that you need to protect from this significant risk.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Watch Out for the Statutory/Governmental Exclusion and Any Restriction on Paying Ransom Demands for Malware Attacks

By Norton Cutler on October 15, 2019

This author has previously discussed the inevitability of security hacks and attempts to require companies holding third-party data to pay some type of damages to the alleged victims of a hack. Even though damage from such hacks is often hard to prove, those who claim to have been victimized and their lawyers, who often operate on contingencies, will continue to file lawsuits that often result in the imposition of at least defense costs and, at times, of some indemnity payments. Hacked companies also suffer actual damage from loss of customers when the hacks are reported as required by multiple laws. Companies should thus take reasonable precautions against data breaches. But if a company takes such reasonable precautions, it should be able to buy insurance for the inevitable hack that actually provides coverage for resulting defense expenses, indemnity payments, and loss of business income.

As discussed in previous columns, there is a project called Cyber Catalyst whereby insurance companies, brokers, and tech companies are trying to set up some type of certification for security products, which seems necessary if insurance companies are going to insist that insureds take reasonable precautions. [https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600] Thus, an insured who follows the certified procedures and also buys a cyber policy should receive coverage for a security hack without any real questions from the carrier. The coverage should include reimbursements for damages from loss of reputation and business because of the hack, which may well be more than any actual damage award payable to those whose information was compromised. Yet, most cyber policies contain the following exclusion for statutory violations and governmental actions:

> This insurance does not apply to any damages, loss, cost or expense in any way related to any claim made or proceeding brought by or on behalf of any governmental authority.

Given that most hacks cause no real damage, violations of the numerous statutory regulations relating to unauthorized access to private or confidential third-party information, including the European GDPR, the California CCPA, and other similar statutes, constitute the most common claims asserted in lawsuits resulting from hacks. Many of these statutes and regulations impose liability without requiring any showing of negligence or other wrongdoing by the hacked company. This above exclusion thus significantly limits the coverage provided by policies that contain it because the **only** claims made often are made pursuant to governmental authority. Insureds purchasing cyber coverage therefore should try to have this exclusion deleted, or buy optional coverage such as the following for claims relating to statutory violations and governmental activities.

> Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for civil fines or civil penalties imposed against such **insured** by order of a regulatory authority having jurisdiction caused by an **act** that results in a **privacy data breach** that first occurs during the policy period.
>
> This Additional Coverage applies only if:
>
> • such actual or suspected injury is not excluded under any section of this contract; and
> • such fines or penalties are reported to us in writing within 60 days of the date the fines or penalties are imposed.

As evidenced by the numerous lawsuits about the breadth of the exclusion for statutory violations and governmental actions, buying any possible coverage for statutory violations and governmental lawsuits is a must for most businesses. [https://blogs.elon.edu/blj/2016/05/16/demystifying-cyber-liability-insurance-what-businesses-need-to-know]

The more significant actual threat to most insureds is malware such as the WannaCry virus or other forms of attack that incapacitate the company's or governmental entity's data. In light of the fact that most companies and many governmental entities are now moving their data to the cloud in order to save on IT costs, coverage for interruption of communication with and access to data stored by third-party providers is becoming an important issue. Experts have also asserted that use of the cloud makes ransomware attacks more likely. Cyber policies do seem to be covering at least some of this risk with the following clause:

> Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for **cyber-threat expense**:

• for a **threat** first made directly against such **insured** during the policy period; and
• paid or incurred by the **insured** within 60 days after receipt of such **threat**.

We will pay for the actual:

• **electronic data recovery costs**;
• **business income** loss; and
• **extra expense**,

you incur due to the actual impairment of your **operations** during the **period of recovery of computer service**, not to exceed the applicable Limit of Insurance for Impairment Of Computer Services – Outside Attack shown in the Declarations.

We will not pay that part of any **business income** loss or **extra expense** you incur to respond to extortion or other similar threat.

These clauses seem to cover at least the expense of restoring data. But this coverage also seems to have some gaps, such as for loss of business income during the outage And now the security companies who created an industry of dubious precautions forced upon all users that generate billions of dollars in revenue, but ultimately achieve less benefit than they cost, have raised a red flag against the simplest and cheapest way of limiting the costs associated with data hacks demanding ransom: paying the ransom demanded to turn on the computer system again. A recent article included quotes from various security experts that insurance companies should not pay ransom demands such as those made against Riviera Beach Florida (which did instruct its insurer to pay) because making payments only provides incentives for further—and repeated—malware attacks, and because even making payments does not guarantee that any, or all, data will be restored. It certainly does seem that, at least if data is properly backed up, there should be an easy and cost-effective way to restart a computer system infected by malware, and if that is not possible, insurers should be able to pay the ransom as the most cost-effective solution to restore use of ransomed computer systems.

Under a theory of pooling of risk and maximizing deterrence, insurance companies or maybe even the government should develop a solution other than paying ransom, but paying still should be allowed if nothing else works. Setting up a fund supported by insurance companies as a group, or a government fund, to compensate for the cost of recreating databases might also solve the problem. This might be similar to the uninsured motorist fund, the vaccine fund, or the wildfire fund recently passed by California, as well as to other no fault methods of compensation. All of these funds pay for damages caused through no fault of the insured, which is really what happens with most of ransomware incursions. Although security companies typically try to blame

someone to pad their consulting revenue, malware issues are mostly impossible to avoid and should be covered by some type of insurance or compensation fund.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

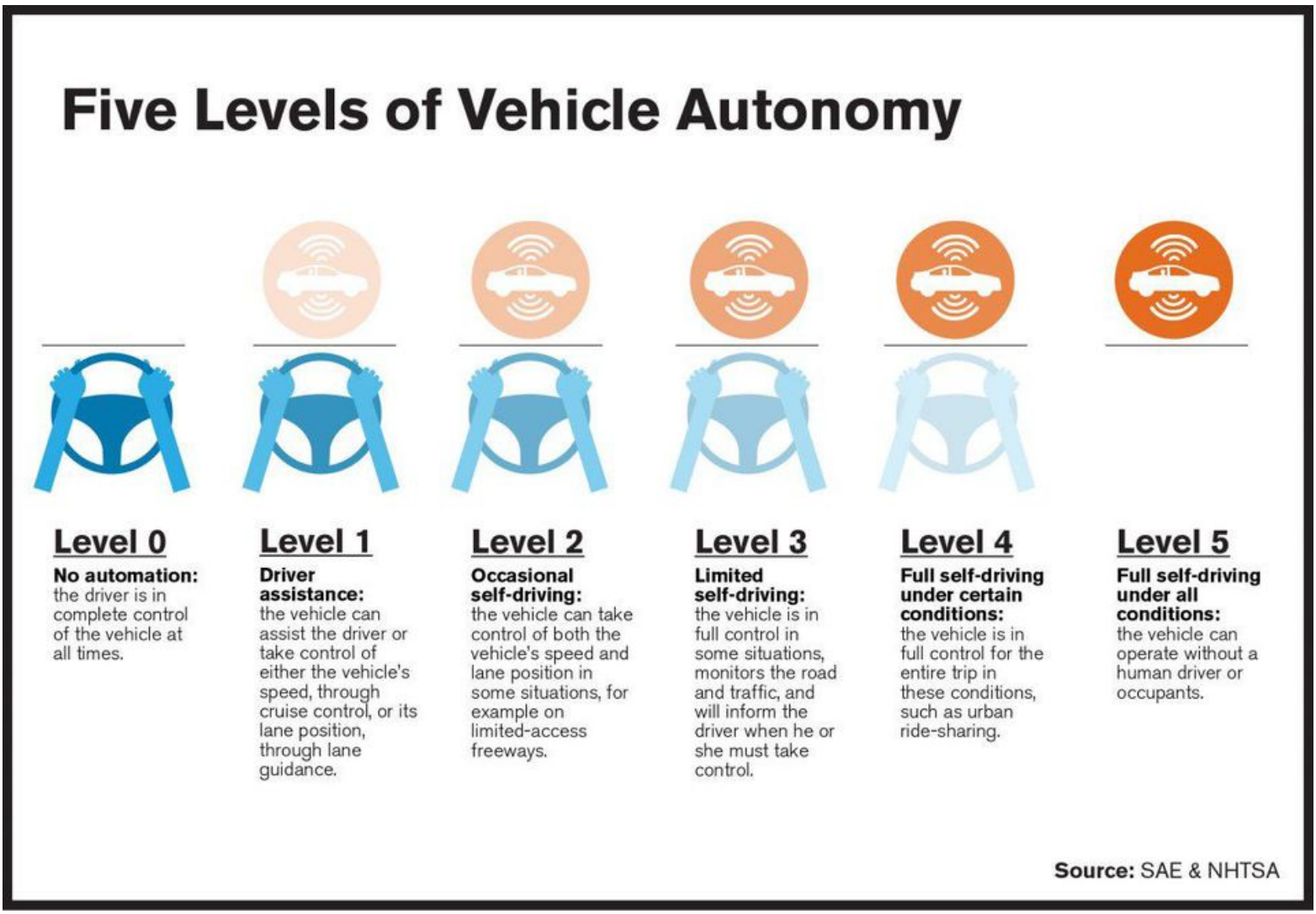
Self-Driving Cars Coming to a Store near You!

By Jay Rossiter on October 8, 2019

Why is this technology so exciting?

The National Highway Traffic Safety Administration (NHTSA) has noted that 94% of auto accidents are attributed to some form of human error on the part of drivers. In 2014, there were an estimated 1.25 million deaths worldwide due to vehicle crashes. There is a potential for autonomous vehicle technology to dramatically re-shape these statistics. The Insurance Institute for Highway Safety anticipates that there will be 3.5 million self-driving vehicles on US roads by 2025 and 4.5 million by 2030.

The Society of Automotive Engineers (SAE) created a six-level scale describing the different levels of vehicle automation. This scale was adopted by NHTSA. Starting with level zero (no automation), and ending at level 5 (full automation), the degree of required driver interface diminishes.



While the advances in technology will serve to decrease accidents, the risks for autonomous vehicle businesses will not disappear, but rather, will shift as those advancements move the market from level to level.

What are the emerging risks?

The insurance industry itself has estimated that by 2025, there will be a decline of $25 billion in auto insurance premiums. But insurers also predict that new lines of coverage relating to the shifting targets of liability will generate $81 billion in premiums—substantially more than the loss from the personal auto insurance market. (*See* Accenture, "Insuring Autonomous Vehicles—an $81 Billion Opportunity between now and 2025" (2017). **https://www.accenture.com/us-en/insight-autonomous-vehicles-opportunity-insurers**

Here are the issues insurers see driving insurance related to autonomous vehicles in the future:

First, cyber security issues will be increasingly important. This includes auto theft by hacking or the failure of smart technology. The recent case against Jeep is an illustration. *See Flynn et al. v.*

FCA US LLC et al., Case No. 15-00855 (S.D. Ill. Aug. 4, 2015). In 2015, a class of 220,000 Jeep owners was certified by a federal court in Illinois. Hackers remotely took the wheel of a Jeep in a controlled test, and the plaintiffs in the lawsuit alleged that they overpaid for their vehicle because it could be hacked through the infotainment system. The takeaway here is that even though technology and security will improve, so will the sophistication of hackers.

Second, the industry anticipates more complex and sophisticated forms of product liability claims arising from the technology, including claims relating to disruption in communications and internet connections, algorithm defects, lidar/radar failure, and camera-vision failure. In *Lommatzsch v. Tesla*, Case No. 18-00775 (D. Utah, Sept. 4, 2018), for example, a lawsuit was filed in 2018 after the plaintiff's Tesla collided with cars stopped on a highway after the autopilot system apparently failed to brake. The plaintiff sued not only Tesla but also a third-party service center on grounds that the center negligently serviced the car when it replaced a sensor prior to the crash.

Third, insurers expect risks arising from new forms of infrastructure investment needed for vehicle-to-vehicle and vehicle-to-infrastructure communication failures, cloud issues, satellite issues, and/or disruption. As cities invest in smart technology to improve traffic logistics and safety, there will be tremendous opportunities for autonomous vehicle businesses, but also shifting risks, particularly with respect to cyber issues.

The bottom line is that if you are a software developer, manufacturer of component parts, or the owner of a fleet of autonomous vehicles, more of the liability in future damage claims will be allocated to you along with the end-product manufacturer.

How does a business in the autonomous vehicle space protect against these emerging risks?

Here are some suggestions:

1. Pay careful attention to warnings, labels and instructions—particularly for manufacturers—as well as to statements within your marketing materials.
2. Broadly use of indemnification agreements from vendors and subcontractors, including dealerships, repair/installation facilities, etc. Such agreements are invaluable, but only go so far, as an indemnity is only as strong as the financial well-being of the company making the promise.
3. Require vendors to carry robust forms of insurance and insisting that you be included as an additional insured where possible. Insist on highly rated insurance carriers, and make sure

to obtain a copy of the applicable endorsement as well as the certificate of insurance, both showing that you are protected.

4. Obtain state-of-the-art insurance that addresses the emerging risks, and pay careful attention to new endorsements that may provide additional protection as they are developed (and equally to endorsements that may limit coverage in those emerging gray areas). Cyber insurance, enhanced product liability insurance, technology errors & omissions coverage, as well as contingent business interruption protection will each be important, depending upon your business and where your business fits into the autonomous vehicle space.

Note also that even though liability risks created by autonomous vehicle systems will shift liability away from drivers to manufacturers, (*see, e.g.*, Munich Re, "Autonomous Vehicles," at 7) **https://www.munichre.com/us/property-casualty/knowledge/expertise/knowledge-publications/autonomous-vehicles/index.html**, ultimately, regulations and legislation in this space will also have a significant potential impact on how risk will be allocated. For example, in the UK, legislation in the form of the Automated and Electric Vehicle Act makes the owner of an autonomous car responsible for certain risks—for example, requiring owners to keep vehicle software up to date and well maintained. It will be essential to track the rules and guidelines for both testing and commercial deployment of autonomous vehicles that are being considered in the US by the Department of Transportation and NHTSA, as well as the legislation being enacted on a state-by-state basis.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Issues With Vendor Certificates of Insurance

By Catherine Del Prete on September 30, 2019

Your company receives a demand letter and you realize that the claim stems from a vendor's product or service. What do you do next? The first step for most companies will be to review the operative contract for any indemnification provisions. Next on the list will be to review any certificates of insurance issued by the vendor. All too often, however, companies at this phase learn that they were never actually added as additional insureds to their vendors' policies or that their vendor's coverage is inadequate.

Certificates of insurance are summaries of insurance coverage. They do not confer any rights on the certificate holders; instead they merely set forth the types and limits of coverage held by the policyholder. As noted in our **blog post** on these issues, a best practice is to request a copy of your vendor's complete insurance policy and all endorsements. Vendors often balk at requests for copies of their insurance policies in the wake of a claim, making it all the more important that your vendor contracts require vendors to produce complete insurance policies. See **this post** for additional tips on drafting vendor contracts.

It is essential that you take the time to review vendors' certificates of insurance when you receive them. Be sure to confirm that the certificate of insurance reflects the types and limits of insurance to satisfy the vendor's insurance obligations under its contract with your company. Also be careful to confirm that the policy period is long enough to provide coverage during your company's relationship with the vendor, and any applicable statute of limitations for claims that could arise from the vendor's work. If not, create calendar reminders 45 days before the vendor's policy period expires to obtain new certificates of insurance (and copies of renewed policies) to ensure no gaps in coverage.

You should also review the listed coverages to confirm that, where possible, it is provided on an "occurrence" rather than a "claims-made" basis. Occurrence-based policies generally provide coverage for an incident that occurs during the policy period, regardless of when the claim was

actually brought. Conversely, claims-made coverage only applies when a claim is made during the policy period.

Finally, and perhaps most importantly, confirm that your company actually has rights to the vendor's insurance coverage. Certificates of insurance typically include vague statements that say things like "Certificate holder is an additional insured where required by written contract" or "Policy includes broad-form vendor additional insured coverage." Coverages granted by additional-insured and vendor endorsements vary greatly. At the very least, request copies of any additional-insured endorsements as well as any significant exclusions. If the vendor objects, request that, at minimum, they list all relevant form numbers on the certificate of insurance. But keep in mind that only the actual policy documents (which should be reviewed carefully if they are provided to confirm adequate coverage) will ultimately determine whether and how much coverage you have under any vendor's policy.

While there is no guarantee of coverage from a certificate of insurance, having processes in place to review certificates of insurance as they are delivered will help protect your company in the event of a claim.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

How Does Your Company Transfer Risk in Its Technology Transactions?

By John Hardin on September 19, 2019

Companies enter an array of technology transactions with third-parties that allow vendors access to the Company's source code, customer data, employee information, cybersecurity measures, and other critical data and infrastructure. These relationships inevitably increase the potential of a cyber attack impacting the Company through an attack against the vendor.

Most technology transactions require the vendor to comply with industry standard cybersecurity protocols and employee training, and to indemnify the Company should the vendor incur a cyber event that impacts the Company. However, those remedies rely on the vendor to maintain industry standards on a going-forward basis (which many do) and to have the financial wherewithal to indemnify the Company (and others) after the vendor suffers a cyber event (which the vendor may or may not have).

Companies therefore should also evaluate which vendors they should require to have a robust cyber insurance policy, and whether the Company should be added as an additional insured. Obvious choices are vendors that have some role in the Company's cybersecurity program, and ones that possess or have access to significant amounts of PII or other critical and confidential Company data. But Companies should also consider whether to require strategically important vendors to procure coverage to protect against an uninsured cyber event causing the unexpected loss of that vendor and resulting disruption to the Company's business.

If a Company decides to require a vendor to obtain cyber insurance, simply including a contractual requirement that the vendor do so may not result in coverage that adequately addresses the risks the particular vendor is most likely to face or impose on the Company, or covers the damages that concern the Company the most. There is no single cyber insurance policy that is predominantly used. Instead, approximately 75 carriers write their own individual cyber insurance policies with differing provisions (sometimes vastly differing provisions), and

many aspects of those policies can be negotiated. Thus, unlike with respect to CGL, worker's compensation, or other traditional policies, a contractual requirement that the vendor obtain a cyber policy with certain limits does not carry the same certainty of protection that it would be expected to do for more traditional policies.

Instead, Companies should consider contractually requiring a specific cyber policy, or specific cyber policy provisions, that adequately addresses or address both the risks to the Company should the vendor suffer from a cyber event and the potential cyber risks applicable to the vendor, including, for example, employee negligence. Likewise, Companies should follow up on the contractually imposed requirement to procure cyber insurance and consider whether they should request and review a copy of the policy the vendor procured, or even require approval of a vendor cyber policy before it is bound.

Lastly, depending on the access granted to the vendor, Companies should discuss whether to include some or all of their vendors in their insurance programs. If one or more vendors are to be added, Companies should discuss with their risk managers and brokers ways to obtain insurance that would provide coverage when the vendor suffers a cyber event, including cyber events allegedly resulting from employee negligence or the failure of the vendor to comply with industry standard cybersecurity protocols.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Insurance and Mergers & Acquisitions

By Michael Sharkey on August 29, 2019

A merger, acquisition, or other corporate transaction can raise a number of issues for the insurance coverage of the parties involved. The transaction may affect the parties' current coverage and their rights under their historic policies. The parties will want to specify clearly the intended interplay of other aspects of the deal, such as indemnities, with available insurance. And the parties may wish to consider purchasing various types of insurance for aspects of the deal itself.

This post provides an overview of insurance-related issues that tech companies (and others) contemplating a corporate transaction should consider and address to avoid gaps in coverage, unpleasant surprises, or unnecessary disputes:

Corporate Transactions Can Affect Existing Insurance Coverage

Many insurance policies require notification to the insurance company if the policyholder under an existing policy undergoes a change in control, or acquires another company above a certain size. These events can have other effects as well, including the obligation to pay additional premiums to cover the new acquisition, or the conversion of Directors & Officers or other claims-made coverage to "run-off" at a change of control, which changes the scope of coverage as further discussed below.

In a corporate transaction, both the target company and the purchaser should review their insurance policies to determine whether the planned transaction triggers any such requirements, so as to maintain continuity of coverage and avoid gaps in protection.

A Change of Control May Require the Purchase of "Tail" Coverage

Directors & Officers insurance policies typically have a "change-of-control" provision that converts coverage to "run-off" if the policyholder is acquired, or otherwise undergoes a change of control.

That is, there is no coverage for any claims arising from conduct taking place after the change of control, and claims based on conduct from before the transaction are covered only if the claims come in before the end of the current policy period. The company will need to purchase new coverage (or be integrated into the policies of its new parent) to have coverage for claims based on post-transaction conduct. These going-forward policies, however, will not cover claims arising out of pre-transaction conduct.

Given that most causes of action are subject to a multi-year statute of limitations, this creates the potential for a gap in coverage in situations where a claim comes in after the transaction alleging pre-transaction wrongful conduct, and the policy period of the target's pre-transaction D&O policy has expired. To close this gap, the target company can purchase "tail" coverage, often as an endorsement adding an "extended reporting period" to its existing policy, extending coverage for pre-transaction conduct to claims coming in for several years.

Change-of-control provisions are most commonly found in Directors and Officers liability policies, but may appear in other types of claims-made policies as well. Parties to a transaction should carefully review the target's insurance policies to determine which would need tail coverage to avoid a gap in coverage after a change-of-control transaction.

Purchasers Should Consider How A Target's Insurance May Respond to Its Particular Exposures

Transaction documents often disclose, and make representations about, a target's current insurance policies, as well as the policies in effect in the last few years. Whether a target has adequate current insurance is an important consideration, but, depending on the target's particular exposures, the purchaser also should consider whether there is additional insurance coverage that should be reviewed, as well as how the transaction may affect that insurance. For example, is the target involved in long-running litigation that already has been noticed under liability policies in effect many years ago, and will the transaction affect the right to access that insurance?

Even if there is no present litigation, long-term latent injuries can trigger "occurrence"-based liability policies dating back many years, through the entire injury process. If the target may face this kind of liability exposure, the purchaser should determine whether it has historic liability insurance policies that may provide coverage, and whether the transaction will affect the rights to access that coverage.

Transactions May Affect the Rights to Access Historic Insurance Policies

“Occurrence”-based general liability policies respond to liabilities arising out of harm during their policies periods, even if the claim for that harm was not made against the policyholder until a later policy period. This is a particular issue with latent injury claims, but even for abrupt accidents, claimants often have multi-year statutes of limitations before they must bring their claims. Thus, a claim may come in after a transaction that alleges pre-transaction harm which would trigger a pre-transaction general liability policy. A frequent question that arises is whether rights to the proceeds of pre-transaction liability insurance for such claims have transferred in the deal. The answer can depend on the language and structure of the deal, as well as how the state law applicable to the insurance policies interprets the “anti-assignment” clauses found in many policies, and these issues should be considered in structuring transactions and evaluating existing and historic policies of the target.

Parties Should Consider the Interplay of Insurance with The Indemnities in the Transaction Agreement

Transaction agreements for corporate transactions often contain provisions in which one of the parties agrees to indemnify the other in various situations. The parties should consider whether they intend these indemnities to be excess to any insurance maintained by the indemnified party that may apply to the same loss. Expressly specifying in the agreement whether a particular indemnity is meant to be net of insurance will help avoid unnecessary disputes on this point after a loss arises.

An Acquirer Placing Its Own Personnel as Directors or Officers of A New Acquisition Should Examine the Interplay of the Multiple Lines of Insurance And Indemnity

While many purchasers will integrate a new acquisition into the acquirer’s own insurance program, this is not always the case. Private equity firms, for example, typically maintain separate insurance programs from their portfolio companies. As a result, if such a firm places its own personnel as a director or officer of an acquisition, that individual may be covered under two separate sets of Directors & Officers insurance policies—that of the acquirer and that of the acquired company. In addition, there may be multiple indemnifications available if that individual is sued.

Which line of insurance or indemnity responds to a given claim against such a director or officer may depend on how the claimant characterizes the individual’s role and alleged misconduct, as well as any language of policies setting out an order in which they respond. Companies should examine the interplay of the multiple sources of insurance and indemnity that may apply in such situations before a claim comes in, to make sure the arrangements reflect the parties’ intent, and that there are no gaps in coverage.

Parties to such an arrangement also should review the portfolio company's Directors and Officers liability policies to make sure they do not contain overbroad "capacity exclusions" that bar coverage for claims arising out of allegations that the director or officer was acting in any capacity other than as a director or officer of the portfolio company. It is not uncommon for claimants to allege directors and officers in this situation acted wrongfully precisely because of their dual roles with both the private equity firm and the portfolio company. An overbroad capacity exclusion could have the effect of barring coverage for such claims by the very fact that the allegations are that the individual was acting in two capacities.

Parties Can Purchase Insurance Policies for Aspects of the Transaction Itself

In addition to considering the effects of a deal on present and historic insurance coverage rights, parties to a transaction can also purchase various types of insurance policies for aspects of the deal itself. Representation & Warranty insurance covers breaches of representations and warranties made by the seller and can provide flexibility in addressing the indemnification obligations in a transaction. An overview of Representation & Warranty insurance appears **here.**

Certain types of transactions may call for specific other types of insurance, including environmental impairment liability policies, political risk policies, and policies that cover the failure to qualify for expected tax or regulatory treatment.

Given the many insurance issues that arise in connection with corporate transactions, parties planning a transaction should carefully consider the effects it will have on the parties' existing insurance, as well as any insurance arrangements that should be made as part of the deal itself. Experienced insurance coverage counsel can assist the parties in addressing these issues.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Recent Developments in Coverage for Email-Based Computer Fraud

By Jeff Bowen on August 22, 2019

As previously reported here, (Nov. 8, 2017), companies falling victim to electronic impersonation ("spoofing") schemes have frequently turned to "computer fraud" coverage found in typical crime policies. In this type of fraud, someone impersonates a vendor, contract partner, or company executive via email or other electronic means, and directs the transfer of funds to an account connected to the fraudster. Courts adjudicating insurance coverage actions arising out of these schemes have reached quite disparate results, with some decisions affirming coverage and some finding no coverage because the loss does not "result directly" from the "use of a computer" or because certain exclusions apply. Since our last update, several more decisions have been issued with potential implications for policyholders pursuing coverage or renewing crime policies. These recent decisions have generally affirmed that spoofing schemes fall within standard computer fraud coverage, though courts have also been willing to apply targeted exclusions for data entry or fraudulent transfers in policies that have them. Purchasers should therefore pay particular attention to any such exclusions in their policies.

A district court in New Jersey recently held that an insured stated a claim for relief under the policy's "computer fraud" coverage after someone had impersonated a Thailand-based vendor through substitution of email domain names and had directed payment to an account operated by the imposter. *Childrens Place, Inc. v. Great Am. Ins. Co.*, No. 18-11963 (ES) (JAD) (D.N.J. Apr. 25, 2019). The fraudsters also accessed and altered an electronic "vendor setup form" so that it provided false payment instructions. The insurer argued that the imposters did not have "direct access" to the computer system, as required under the insuring agreement, and that the fraud did not "directly cause" the transfer of money from the insured's account to an account outside its control because of the independent acts undertaken by employees. But the court was persuaded that the complaint alleged sufficient facts to constitute both direct access by the impersonators and a direct causal link to the transfer.

The Second Circuit similarly affirmed coverage under a computer fraud provision, which applied to the "fraudulent . . . entry of Data into . . . or change to Data elements or program logic of . . . a Computer System." *Medidata Solutions Inc. v. Fed. Ins. Co.*, 729 Fed. Appx. 117 (2018). The insured argued that someone had fraudulently entered data into Medidata's computer system by using code to cause an email address to appear as that of the company's president, along with the company president's photo. The court held that the "unambiguous language of the policy covers the losses" because the imposters "crafted a computer-based attack" that created messages that appeared to be from high-ranking company officials. The attack met the policy criteria because the email's appearance was "altered by the spoofing code to misleadingly indicate the sender." The court also applied New York's proximate cause standard and held that the insured had suffered a direct loss, noting that any independent acts taken by employees to effectuate the transfer were not "sufficient to sever the causal relationship between the spoofing attack and the losses incurred."

Similarly, the Sixth Circuit found coverage for a manufacturer who fell victim to an imposter posing as a vendor. *Am. Tooling Ctr., Inc. v. Travelers Cas. & Surety Co.*, 895 F.3d 455 (6th Cir. 2018). The fraudster directed payment to be made to a different bank account through a series of emails to the company's vice president. The court agreed with the insured that the payments constituted "direct loss" because the policyholder "immediately lost its money" when it transferred the funds, and "there was no intervening event." Moreover, the loss satisfied the "use of a computer" component of the "computer fraud" provision because the imposters "sent [the insured] fraudulent emails using a computer and these emails fraudulently caused [the insured] to transfer the money."

While the reasoning in these three decisions should prove helpful for policyholders seeking coverage for spoofing schemes, two other recent decisions have denied coverage based on exclusions for fraudulent transfers or data entry. A Washington district court upheld an insurer's denial of "computer fraud" coverage after an accounts payable clerk altered the instructions for payment to a general contractor in response to a fraudulent external email. *Tidewater Holdings, Inc. v. Westchester Fire Ins. Co.*, No. C18-6006 BHS (W.D. Wash. May 31, 2019). Although the court concluded that the scheme fell within the coverage grant, the court also found that an exclusion for "loss resulting from any Fraudulent Transfer Request" applied to the claim. The policy defined "Fraudulent Transfer Request" as "the intentional misleading of an Employee, through a misrepresentation of a material fact which is relied upon by an Employee, sent via an email, text, instant message, social media related communication, or any other electronic . . . instruction." The court rejected the insured's argument that application of the exclusion was ambiguous as applied to different coverage sections. Furthermore, unlike the exclusions

discussed in the blog update of January 8 of this year, the exclusion at issue here was not limited to “physical” loss.

Addressing another case filed in Washington district court, the Ninth Circuit upheld the denial of coverage for a fraudulent scheme that caused company employees to alter wiring instructions and to send four payments to a fraudster’s account. *Aqua Star (USA) Corp. v. Travelers Cas. & Surety Co. of America*, 719 Fed. Appx. 701 (9th Cir. 2018). Although the court assumed without deciding that the policy generally covered that type of “computer fraud,” the court focused on an exclusion for “loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured’s Computer System.” The court noted that the employees plainly had authority to access the system and had entered the data causing the loss.

Overall, these recent cases provide strong support for placement of spoofing and similar schemes within the general parameters of computer fraud coverage. At the same time, coverage for this type of loss under any particular crime policy will depend upon the existence and precise wording of any exclusions for fraudulent transfers or data entry. As ever, purchasers of crime policies should scrutinize the potential scope of any such exclusion.

Children’s Place
Medidata
American Tooling
Tidewater
Aqua Star

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Representation and Warranty Insurance Coverage for Corporate Transactions

By Michael Sharkey on August 12, 2019

It is becoming increasingly important for tech companies considering a merger, acquisition, or other corporate transaction to understand the use of Representation & Warranty Insurance ("R&W Insurance"). R&W Insurance is a type of insurance policy purchased in connection with corporate transactions; it covers the indemnification for certain breaches of the representations and warranties in the transaction agreements. It is designed to provide additional flexibility in addressing these obligations by, for example, reducing or eliminating the need for an escrow by the Seller.

The use of R&W Insurance is becoming more popular, and the volume of R&W Insurance sold has increased considerably in recent years. Recent estimates suggest it is now used in over 30% of North American transactions, with over 3,000 policies placed in North America in 2018.

R&W Insurance can be purchased as either Seller-Side or Buyer-Side coverage. Seller-Side coverage is a form of liability policy, covering the Seller's liability for claims of breach of a representation or warranty. Buyer-Side coverage is a form of first-party coverage, directly compensating the Buyer for alleged breaches by the Seller. One common variation is a Buyer-Side policy that also protects the Seller (by barring the insurance company, except in cases of fraud, from pursuing the Seller after the insurance company makes a payment to the Buyer for a breach). This variation is often used to reduce a Seller's escrow or other exposure to representation and warranty claims, while still providing a source of recovery for the Buyer in the case of breach.

A key point in negotiating R&W Insurance is the amount of the limits and retentions. Limits are often set at 10% of enterprise value, with retentions typically 1% of enterprise value. Premiums generally range from 2% – 4% of limits, with one estimate placing the average premium at less than 3% of limits. The responsibility for the amount within the insurance policy's retention is often

split between the Buyer and the Seller, in the form of a deductible in the transaction agreement, but an increasing number of transactions have provided that the Buyer bear the entire retention amount, with recent estimates suggesting that between one-quarter and one-third of R&W Insurance transactions in 2018 included no seller indemnity.

There are several ways R&W Insurance can benefit a Buyer. In an auction situation, it can make a bid more attractive by reducing the Seller escrow, while still providing the Buyer with protection. The Buyer can purchase insurance to cover higher amounts than the cap the Seller is willing to accept, and with longer survival periods (generally three years for general representations and six years for fundamental and tax representations, although some policies are sold with a six-year policy period for all breaches). R&W Insurance can also provide a mechanism for recovery when pursuing the Seller or Sellers is expected to be difficult (for example, if there are numerous Sellers, or if the Seller is located in a foreign jurisdiction, may be insolvent, or has stayed on in the target's management).

Buyers should be aware, however, that R&W Insurance does not provide as broad coverage as a Seller escrow of the same size, and so is not a perfect replacement. R&W Insurance does not cover breaches known to the policyholder (which must be disclosed), so if the Buyer, for example, has particular concerns about the way the Seller has been handling a tax issue, R&W Insurance coupled with a tax representation is not the solution. In addition, there are certain standard exclusions (including for forward-looking statements, working capital adjustments, asbestos or PCBs, and underfunded pension liability), and the insurance company will perform a detailed underwriting and may add deal-specific exclusions directed at high-risk areas for the target or its industry.

Indemnification from an escrow, by contrast, is not limited to breaches of representations and warranties, but can also include breaches of covenants and special indemnities; these would not be covered under an R&W Insurance policy. Thus, to the extent R&W Insurance is used to replace part of the Seller's escrow, the recovery available to the Buyer will not be as broad. The insurance also involves payment of a premium and an upfront underwriting fee, and will have a retention that leaves some of the risk on the Buyer.

R&W Insurance is typically used to reduce or eliminate the need for an escrow from the Seller, allowing more of the proceeds to be distributed right away. It can provide a cleaner exit for the Seller, with fewer contingent liabilities. It may also be purchased to protect a passive or minority investor that was not in direct control.

The underwriting process to purchase R&W Insurance can be as short as seven days, though the initial phase of the effort can start much earlier. The first stage of the process involves working with an insurance broker to provide basic information and drafts of the transaction documents to one or more insurance companies. The insurance companies then provide non-binding indications of the coverage they would be willing to provide, with premium estimates. If the parties proceed, there is a non-refundable underwriting fee (usually between $25,000 and $60,000) for the insurance company to proceed with its diligence. After it has performed its diligence, the insurance company will provide a draft insurance policy, and this is often followed by some negotiation over the coverage.

A key issue for counsel representing that policyholder is coordinating the retentions, definitions of loss, and subrogation clauses in the R&W Insurance to match the purchase agreement, and the parties' intent as to the risk borne by each party in different situations. Counsel also can assist in pushing back to seek to limit or eliminate the deal-specific exclusions the insurance company proposes after the diligence process. Counsel may be able to provide additional information enabling the insurance company to become comfortable enough with a particular issue to remove a proposed exclusion. Failing that, counsel should negotiate the precise language of each exclusion, so that its reach is no broader than the specific issue that was identified during diligence. Other features of the policy may be subject to negotiations, as well, and experienced counsel likely already has a set of negotiated enhancements to most insurance companies' basic standard R&W Insurance forms that they have developed in previous deals.

R&W Insurance is not the only insurance relevant to M&A transactions. Certain types of transactions may benefit from other types of insurance, including environmental impairment liability policies, political risk policies, and policies that cover the failure to qualify for expected tax or regulatory treatment. In addition, an M&A transaction may affect the target's existing or historic insurance program in various ways. An overview of other insurance issues in corporate transactions can be found **here**.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Will Your Cyber Insurance Actually Pay Claims?

By Norton Cutler on August 1, 2019

I have several times discussed the need for cyber insurance that will actually cover reasonable claims; a need that still seems to exist. The case of *Hub Parking Technology USA v. Illinois National Insurance Company* (**https://www.law360.com/articles/1170778/parking-tech-co-says-aig-must-defend-it-in-privacy-row**) that was brought in Pennsylvania District Court in June of this year illustrates this problem. Hub bought security and privacy insurance that was intended to cover security breaches and disclosure of personal data in violation of privacy rules. Hub was then sued in underlying litigation for printing parking receipts at the Cleveland Airport that showed eight digits of credit card numbers instead of the standard last four digits permitted under various state statutes and case law. When Hub submitted the claim to its cyber insurer, the cyber insurer rejected the claim based on its conclusion that there had been no loss of privacy or security information, as well as on several exclusions, such as those for contractually assumed liability and intentional acts. Although the insurer may have had a legitimate complaint that there really was no damage from this alleged violation (and the plaintiffs had not alleged that anyone suffered actual damage or identity theft arising from the parking receipts at issue; they rather relied on an FTC study showing that similar incidents have caused actual damage, so that the potential for damage existed), that should not have prevented the insurer from providing at least a defense.

But instead of defending Hub, the insurer drafted two denial letters setting forth the weak excuses that the underlying complaints contained no allegations of a security breach or a loss of privacy, based on the lack of custody by Hub of the data and of direct complaints from the consumers (Hub was brought into the pending consumer class action against the parking company, SP, through a third-party complaint by SP against Hub, the provider of the receipts at issue). Any reader of the complaints could easily have concluded that they alleged both a breach of the security of the credit card numbers and a loss of privacy and confidential data on the part of customers whose cards had eight numbers exposed. But rather than applying this common-sense reading and simply honoring the policies it had issued by providing a defense

because the complaints alleged potentially covered conduct, the insurer crafted a series of hyper-technical excuses including, as mentioned above, the contract and intentional act exclusions.

This insurer conduct again highlights the need for cyber policies—and cyber insurers—that actually pay when there is a cyber breach. According to the pleadings and allegations in the third-party complaint against Hub, Hub did not intentionally fail to comply with the rules about credit cards receipts, it simply forgot and failed to execute on meeting the requirement in its contract. That is what companies buy insurance for: an accidental failure to do something. Of course, the class-action complaint alleged intentional misconduct, but Hub's notice denied intentional wrongdoing and alleged that the failure had been negligent at best; moreover, SP's third-party complaint against Hub alleged negligent violations of the contract between SP and Hub. Under those circumstances, this appears to be a basic case where at least the duty to defend is obvious, but the insurer nonetheless tried to avoid providing the required defense.

Real cyber insurance is needed to cover the numerous instances where lawsuits occur even though no one suffers any monetary harm. A recent lawsuit filed against the University of Chicago for cooperating in a research project using deidentified medical data to seek a cure for cancer (**https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html**) also illustrates the baseless nature of many of these cases, which still have to be defended by insureds—and hence their insurers who have a duty to defend. The GDPR fines of 185M pounds imposed on British Airways (**https://www.nytimes.com/2019/07/08/business/british-airways-data-breach-fine.html?register=email&auth=register-email**) and of over 200m pounds imposed on Marriott Intl. (**https://www.wsj.com/articles/marriott-faces-123-million-fine-over-starwood-data-breach-11562682484**) even though no one suffered any monetary harm from the hacking also demonstrate that policyholders can be subject to significant fines even when there is no actual monetary damage. Similarly, Equifax has recently announced that it is subject to a fine of $650m for its data breach even though, according to the NYT, security experts cannot point to any actual fraud against Equifax customers or to the appearance of customer data on sites where such data is normally traded. (**https://www.nytimes.com/2019/07/22/business/equifax-settlement.html**) Many cyber policies exclude fines by governmental agencies, and it seems insureds should seek coverage for this type of regulatory activity that seems inevitable. Insurance against the new spate of biometric and location data lawsuits would also seem necessary.

The recent announcement by Lloyd's that its members need to clarify whether policies cover cyber incursions shows the need for clarity in cyber insurance policies. Lloyd's apparently fears that vague CGL and property policies might be construed to cover cyber losses and encourages

a simple explanation of what is covered. It might be equally smart for Lloyd's to clarify what is covered cyber policies so that insureds can buy policies that will cover likely breaches. Doing so should help the insureds as much as would a certified set of software protections against cyber incursions that would, as discussed in a previous blog, improve the certainty of coverage, as contemplated by the Cyber Catalyst project.

So far these policies seem more illusion than actual coverage.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Who Gets to Select Defense Counsel?

By Catherine Del Prete on July 16, 2019

A policyholder is usually thrilled when its insurer agrees to provide a defense of a claim. However, all too often, an insurer's position on how that defense is to be provided surprises the policyholder. Sometimes, the policyholder learns for the first time that it does not have the right to select defense counsel. Other times, it learns that it is allowed to select defense counsel but must do so from a list of pre-approved panel counsel. In yet other circumstances, the policyholder is permitted to select its own defense counsel but may be limited to the rates approved by the insurance company (which are sometimes far below what the policyholder's preferred counsel is charging).

To avoid being put in this predicament in the wake of a claim, policyholders should carefully review their policy provisions relating to selection of defense counsel and payment of defense costs. If your company's policy permits the insurer to select defense counsel or limits your choice of defense counsel to a panel counsel list, you may still have options.[1] And if your company's policy gives the insured the right to select defense counsel, be sure to review other relevant provisions that may require the selection to be "mutually agreeable" to both parties or that the insurer consent to the selection by defense counsel. Other policies might give the policyholder the right to select defense counsel but require the insurer only to pay "reasonable attorneys' fees." In these cases, insurers often argue that attorneys' rates are too high and agree to pay only a fraction of the hourly rates.

Carriers are often willing to negotiate pre-approval of preferred defense counsel if the conversation begins before a claim arises. Insurers are able to obtain significant discounts when hiring defense counsel due to the volume of claims that pre-approved counsel receive. As such, your company's insurer may be unwilling to pre-approve your preferred attorneys at their standard rates. Compromises can often be worked out that involve using blended rates (*i.e.*, one rate for all attorneys at the firm, regardless of position) or the policyholder agreeing to pay the delta between the insurer's approved rate and the attorney's actual rate.

In addition, even if the negotiation to retain your preferred counsel occurs after a claim has arisen, some carriers are willing to work with their policyholders when a compelling case can be made. Carriers will consider a variety of factors to determine whether the retention of counsel (and approval of their rates) is reasonable, including the nature of the case, the complexity of the issues, the amount of damages in question, the attorney's expertise and experience, similar rates charged for similar services in the geographic area, and the attorney's institutional knowledge with the policyholder.

Endnote

[1] In certain circumstances, such as claims with covered and non-covered allegations or differences in case strategy, you may be entitled to select independent defense counsel, regardless of the policy language. The specific circumstances of the claim and state law are determinative in these situations.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

CCPA Insurance Coverage Issues: Avoid Gaps in Your Program

By Jim Davis, Bradley Dlatt & Selena Linde on July 10, 2019

CCPA Week Webinar (FREE), July 17, 2019 1:00 p.m. PT

Insurance policies are some of a company's most valuable assets during times of increased risk and uncertainty. Yet, corporate policyholders often leave money on the table by failing to thoughtfully construct their insurance program to respond to the risks inherent in their business and neglecting to properly manage potential insurance claims. In recent years, data privacy and security has become a growing source of corporate risk for businesses and presenting new, evolving challenges for risk managers and insurers.

Starting January 1, 2020, companies doing business in California that meet certain qualifying criteria will be subject to an entirely new sphere of risk, as **California's sweeping Consumer Privacy Act (the CCPA) goes into effect**. The CCPA will apply to any for-profit entity doing business in California that collects personal information about California consumers and meets at least one of three criteria:

1. Has annual gross revenue above $25 million;
2. Annually buys, sells or, for commercial purposes, receives or shares personal information of at least 50,000 California consumers, households or devices, or
3. Derives at least 50% of its annual revenue from selling California consumers' personal information.

Moreover, if a business is subject to the CCPA, its subsidiaries and affiliates may also be covered if they share common branding, including a shared name, service mark or trademark. **For more information about the CCPA, including a diagnostic toolkit to determine whether your business may be subject to the CCPA, click here.**

The CCPA provides extensive protections for consumers with respect to the collection, storage, use and disclosure of a broad swath of “personal information.” A failure to comply with the exacting requirements of the CCPA may expose companies to an enforcement action from the California Attorney General or lawsuits from impacted California consumers. The CCPA carries substantial per-violation statutory penalties.

CCPA’s Likely Impact On Corporate Risk Profiles and Insurance Programs

- Increased data breach costs and volume of data privacy litigation
- Heightened scrutiny of Directors and Officers
- Increased insurance premiums, particularly for cyber risk/liability coverage
- Increased cost of settlements and judgments

Major Forms of Insurance Coverage That May Respond To A CCPA Claim

Cyber Risk/Privacy Policies: Provides claims-made “first-party” coverage for losses due to destroyed/damaged data, business interruption, physical damage and/or cyber extortion and “third-party” coverage for data breach investigations and defense of privacy liability actions.

Professional Liability/E&O Policies: Claims-made coverage for wrongful conduct in connection with the delivery of “professional services.”

Directors & Officers Policies: Provides claims-made coverage for liabilities incurred by directors and officers and/or claims made against a company arising out of the conduct of the company’s directors and officers.

Employment Practices Liability: CCPA’s definition of “consumers” may include employees, leaving open the possibility that employees may bring CCPA claims against their employer. Covers “employment practices” claims.

- Commercial General Liability: Provide occurrence-based coverage for “bodily injury,” “property damage,” and/or “personal and advertising injury.”
- Crime Policies: Covers losses due to crime or dishonesty. Property Policies: Provides coverage for property damage resulting from specific events. Typically also covers loss arising from interruption to a business, whether caused by damage to your property or a business partner’s property

Consider The Scope of The CCPA In Negotiating Your Policies and Preparing For A Potential Loss

A company should never accept an off-the-shelf policy. Instead, companies should seek to customize their policies to fit their risks. With respect to the CCPA, a company's policies must cover more than a data breach or theft. Policies must cover acts arising out of the collection, use, storage and disclosure of "personal information," a term that is defined broadly in the CCPA. Companies should carefully review this statutory definition and think deeply about how the identified forms of "information" interact with their business. Given the broad scope of the CCPA, there is a high potential for corporate exposure. To prepare for this risk, companies must build the right team, keep good insurance records, audit their policies, and have a robust process in place to promptly report insurance claims in the event that the company is facing a CCPA-related investigation or lawsuit.

For more information tune in to the Perkins Coie CCPA Week webinars, including CCPA Insurance Coverage Issues: Avoid Gaps in Your Program on July 17, 2019 1:00 p.m. PT.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

D&O Coverage for Tech Risks – Don't Let the "Invasion of Privacy" and "Professional Services" Exclusions Take You by Surprise

By Robert P. Jacobs on June 25, 2019

Directors & Officers liability insurance—commonly known simply as D&O insurance—is meant to protect corporate directors and officers from, among other things, claims alleging breaches of duty and management failings that adversely affect the value of the company's stock. And any event in which directors or officers are deemed to have had an oversight function could ultimately result in a claim that floats up to the director- or officer-level if the company's stock suffers.

Like all types of insurance, D&O policies begin with fairly broad grants of coverage that are then whittled away by various exclusions. While D&O insurance policies are complex contracts, with numerous exclusions, there are two particular exclusions that might facially appear to not have much relevance to a tech company, but which insurers could assert as a bar to coverage for key parts of the company's operations.

The "Invasion of Privacy" Exclusion.

The first of these is the exclusion of claims for "invasion of privacy." That term is found in an exclusion for claims arising from bodily injury which, to a casual reader, might make sense because directors and officers are not typically accused of physically harming anyone, and coverage for those types of claims can typically be found in a general liability insurance policy. But among the items enumerated as forms of bodily injury is "invasion of privacy," a term that could have significant implications to any company exposed to a high risk of a data breach. Indeed, it could be alleged that a data breach that results in the release of an individual's confidential information—such as medical or financial information, among other things—invades that individual's privacy rights.

The question of what “privacy” means under a liability insurance policy is not, however, entirely clear. Specifically, does it mean a right to secrecy or a right to seclusion? This question is presently under consideration by the California Supreme Court in *Yahoo Inc. v. National Union Fire Insurance Co of Pittsburgh, PA,* in which the policyholder, Yahoo, is seeking coverage under its general liability policy for alleged violations of the Telephone Consumer Protection Act (“TCPA”), a law that is meant to protect consumers from, among other things, unwanted telephone solicitations. Yahoo was alleged to have violated the TCPA by sending unsolicited text messages containing advertisements. Yahoo’s insurer denied coverage for this alleged liability on the premise that an unsolicited text message may violate a person’s right to seclusion (or to be left alone), but that the term “invasion of privacy” in the policy’s coverage grant is meant to refer only to a right to secrecy.

The California Supreme Court is considering this issue because there appeared to be some tension among California appellate court decisions. In reality, as an undefined policy term, a right to privacy should probably be deemed to refer to both a right to secrecy and a right to seclusion. Regardless, many commentators expect the California Supreme Court to rule in the insurer’s favor and hold that the right to privacy in the context of the coverage provided by the policy at issue is meant to refer solely to the right to secrecy.

While the *Yahoo* case provides an interesting view into that debate, the reality is that, if the California Supreme Court rules in the insurer’s favor, D&O insurers may be emboldened to rely on the “invasion of privacy” exclusion with respect to any data breach that releases personal or confidential information and that gives rise to securities and shareholder claims.

Any policyholder that is concerned about the potential for a large-scale data breach that could affect a company’s stock should be aware of this exclusion and attempt to minimize or remove it through negotiation during the insurance underwriting process.

The “Professional Services” Exclusion.

The second exclusion which might be overlooked at first blush is the so-called “professional services” exclusion. This exclusion typically attempts to bar coverage for claims “based upon, arising from, in consequence of, or in any way directly or indirectly relating to the rendering or failure to render professional services.” Insurers include these exclusions in their D&O policies because they believe that such claims are more appropriately covered under professional liability or errors and omissions (“E&O”) insurance policies, which are meant to protect companies against claims alleging negligence or malpractice in the rendering of “professional services” (a term that typically varies in definition depending on the policyholder’s industry).

The flaw in this theory is, again, the reality that any type of claim that causes a drop in a company's stock also could become a D&O claim. The professional services exclusion should, therefore, be of concern to any company that provides a service as part of its core business. For example, a software company that provides installation, troubleshooting, or maintenance services along with the sale of its product is providing a service. If anything goes terribly wrong with that type of service, such as the widespread introduction of a virus or malware, that could result in a professional negligence claim. And, if the problem is big enough to affect the company's stock, it could become a D&O problem. This is even more acute with respect to companies in which the provision of service is their core business, such as companies that provide computer networking or architecture services or that set up blockchains, etc. If anything goes wrong in the provision of such services, and an alleged liability bubbles up to the directors and officers, insurers might raise the professional services exclusion and deny coverage.

Policyholders in the tech industry should be aware of the professional services exclusion and seek to remove it or limit its scope when procuring or renewing their D&O policies. This should be a matter of negotiation. One suggestion is to seek more favorable wording, so that the exclusion bars coverage only "for" professional services claims, as opposed to one that bars coverage for claims "arising out of" professional services. The term "arising out of" is usually construed very broadly under the laws of most states as meaning "but for" causation: for example, but for the negligent rendering of professional services, there would not have been a stock drop. That language could prompt an insurer to assert the exclusion with respect to any claim that has any causal link to a professional service. But if the exclusion relates only to claims "for" the rendering of professional services, then it is possible to argue that any D&O claim is "for" the alleged failure to properly manage the company, not "for" any negligence in the rendering of professional services.

All tech companies should be aware of both of the above exclusions when procuring or renewing their D&O policies. While market factors drive what any given policyholder can accomplish through negotiation, there are reasonable limitations to these exclusions that accomplish their core goals without eviscerating the D&O coverage that the policyholder needs to properly protect its directors and officers.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Lookout for Luddites: Don't Overlook the Risk of a Non-Electronic Data Breach When Evaluating Your Cyber Insurance Program

By Freya K. Bowen on June 17, 2019

In the wake of numerous high-profile electronic data breaches, companies are justifiably concerned about beefing up their cybersecurity programs and ensuring that they have adequate insurance coverage in the event of an electronic data breach. While the unauthorized disclosure of sensitive electronic data, whether through cyberattacks, insider malfeasance, inadvertence, or otherwise, is, of course, a substantial risk that must be addressed in any cyber insurance program, businesses should also understand and insure against their potential exposure in the event of an old-fashioned breach of sensitive information by way of paper or other non-computerized records.

These types of ink-and-paper data breaches happen more often than one might expect, given the media attention paid to electronic data heists. The healthcare industry, for example, is especially plagued by non-electronic data breaches, despite wide-spread adoption of electronic health records. According to a recent study by the *American Journal of Managed Care*, paper and films were the most frequent storage media at issue in data breaches that occurred in hospitals during the study period, whereas network servers were the least common. **Statistics from the Office of Civil Rights Annual Report** to Congress on Breaches of Unsecured Protected Health Information, published by **HHS in 2012**, revealed that paper records were involved in 23 percent of major breaches of protected health information (those affecting 500 or more individuals) and 61 percent of smaller breaches. *See also* **Prevent Breaches: Don't Forget Paper**. This problem has not gone away in the intervening years: 11 major breaches of protected health information reported to date in 2019 involve paper or film records.

Moreover, non-electronic data breaches afflict both large and small organizations. For instance, in 2017, the Memorial Hermann Health System in Southeast Texas, which is comprised of 16 hospitals and specialty services in the Greater Houston area, agreed to pay $2.4 million to HHS

for disclosing a patient's personal health information in a **press release**. On the other end of the spectrum, Cornell Prescription Pharmacy, a single-location compounding pharmacy in Denver, Colorado, agreed to pay a $125,000 fine to HHS for disposing of documents containing patients' protected health information in a **dumpster on its premises**.

Insurance-industry statistics confirm that the risk of a non-electronic data breach is not confined to the healthcare industry. According to Gen Re, the overall number of data breaches involving paper records nearly tripled in **2017**. The 2017 NetDiligence Cyber Claims Study reported that 9% of insurance claims for data breaches arose from **paper records**. The **2018 study** noted that "the mishandling of paper records continues to be an annoying and expensive event," with crisis-services costs ranging from $14 – $197,000 (averaging $30,000) and total breach costs ranging from $600 – $926,000 (averaging $69,000).

Despite the wide-spread aspiration of many businesses to adopt a "paperless office," in reality, most organizations today still utilize at least some paper records in addition to digitally stored data. Moreover, even in the absence of paper-based record keeping, non-electronic data breaches can flow from such things as loose documents left on a desk or printer or printed materials accidentally routed to a dumpster instead of a shredder. In one notable example, an employee left notebooks containing handwritten personal customer information in a backpack in a deli. In short, no business is immune from the risk of a non-electronic data breach.

These types of data breaches may also give rise to regulatory risk. For instance, at the federal level, the Health Insurance Portability and Accountability Act (HIPAA) applies to covered entities' use of protected health information regardless of whether the information is in electronic, paper, or **other form**. Likewise, financial institutions subject to the Gramm-Leach-Bliley Act must comply with the Act's requirements to safeguard all customer information, regardless of whether that information is housed in electronic or **paper form**. At the state level, the sweeping **California Consumer Privacy Act (CCPA)**, which takes effect on January 1, 2020 and applies to certain companies that collect and control personal information of California residents, protects both paper records and electronically stored information. (For more discussion of insurance coverage for alleged violations of the CCPA *see* ***Beyond GDPR: Insurance Coverage for Emerging Cybersecurity and Privacy Regulatory Exposure***). Although many state breach notification statutes apply only to electronically-stored information, many apply more broadly: For example, statutes in **Alaska**, **Hawaii**, **Indiana**, **Iowa**, **Massachusetts**, **North Carolina**, and **Wisconsin** require notice of non-electronic data breaches as well.

As a result, any business seeking to manage potential exposure arising out of data breaches should make sure its insurance program provides coverage for non-electronic data breaches as

well. Although many cyber insurance policies cover both electronic and paper breaches, some policies contain exclusions for losses arising from the theft or disclosure of paper records. If your company's policy contains such an exclusion, you should consider addressing that issue with your broker and carefully evaluate your other insurance policies such as CGL, E&O, D&O, and Crime policies to make sure that the particular risks faced by your business with respect to a non-electronic data breach are adequately covered.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Are Cyber Claims Covered Under Coverage B of CGL Policies?

By Catherine Del Prete on May 31, 2019

The consequences of a data breach can be far-reaching. While the initial issues in the wake of a breach often involve investigation into the cause of the breach and sending notification to those affected (both of which are covered by most cyber insurance policies), coverage for certain types of third-party claims stemming from cyber breaches may be available under Commercial General Liability ("CGL") insurance policies.

CGL insurance policies provide coverage for claims of "Bodily Injury," "Property Damage," and "Personal and Advertising Injury." Bodily Injury and Property Damage claims are covered under Coverage A of CGL policies, while Personal and Advertising Injury claims are covered under Coverage B. This blog post briefly summarizes the major issues policyholders encounter when seeking coverage for Personal and Advertising Injury (Coverage B) under CGL policies that arise out of a cyber incident.

With respect to Coverage B, the 2012 standard ISO form **CGL policy language** provides coverage for "those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury' to which this insurance applies . . . [and] is caused by an offense arising out of your business[.]" Covg. B §§ 1(a)-(b). The policy defines "personal and advertising injury," in relevant part, as "injury, including consequential 'bodily injury', arising out of one or more of the following offenses . . . e. Oral or written publication, in any manner, of material that violates a person's right of privacy . . . ."

Following a cyber breach, third parties often assert claims for violations of their right to privacy, which should be covered under subsection E of the "personal and advertising injury" definition of a CGL policy. However, insurers frequently argue that a cyber breach resulting in the access of someone's personal information falls outside the scope of coverage because no "publication" occurred. Carriers typically focus on two main issues to defeat coverage: (1) whether there has

been widespread disclosure of the personal information and (2) whether the claim requires that the *insured* actually publish the personal information (instead of merely preventing the publishing of the information). Caselaw in this area is scant.

A frequently-cited case on this issue is ***Zurich American Insurance Co. v. Sony Corp. of America*, No. 651982/2011, 2014 WL 8382554 (N.Y. Sup. Feb. 21, 2014)**. There, the New York Supreme Court considered whether class action suits for damages stemming from the **Sony Playstation data breach** were covered under Coverage B of Sony's CGL policy. The court held that there was a "publication" of information when the hack occurred. However, the court also determined that the CGL policy required the *policyholder* to publish the information. Because the hackers were the publishers of the personal information, the court determined that no coverage existed under Coverage B of the CGL policy. Sony appealed, but the case settled before the appellate court issued its decision.

In a more recent case, ***Innovak International, Inc. v. Hanover Insurance Co.*, 280 F. Supp. 3d 1340 (M.D. Fla. 2017)**, the District Court for the Middle District of Florida held that claims stemming from a data breach did not fall within the CGL policy's definition of "personal and advertising injury" because there was no publication of data. There, the insurer argued that that no publication occurred because the personal information was not publicly disseminated and that, alternatively, the insured did not publish any of the information stolen in the data breach. Analyzing the policy under South Carolina law, the court found that the policy required publication by the *insured* for coverage to apply.

As a final note, some CGL policies contain exclusions for claims under the Personal and Advertising Injury coverage that "aris[e] out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information." *See* **ISO Form CG 21 06 05 14**. If your policy has this exclusion, request that it be removed.

While the body of caselaw on the application of Personal and Advertising Injury coverage to cyber claims is still developing, it is clear that coverage will hinge on the specific facts of each case. Ensuring that your company has broad cyber coverage for third-party claims arising from cyber breaches is vital, as is evaluating your CGL and cyber coverages in conjunction with each other to ensure that no gaps exist.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Can There Be a Duty to Defend Intentional Acts on Social Media?

By Jeff Bowen on May 21, 2019

Can an intentional attack carried out through social media trigger liability coverage? A recent Pennsylvania case found potential coverage under a homeowner's policy for a case of cyber bullying that ended in the suicide of the victim. The court found that the intentional actions of the insured's son constituted an accident, and therefore an occurrence, because the claim in part alleged negligence and because the actions of the victim were not necessarily expected from the standpoint of the insured. This specific situation is, of course, unlikely to arise in the context of a businesses concerned about social media risks, but the underlying reasoning may be useful in assessing potential coverage for other intentional acts carried out over social media or other communications technology.

In the general liability context, one of the most frequently litigated issues involves the definition of occurrence, which usually incorporates the idea of an accident. An obviously intentional act by an insured person, such as a direct physical assault, can fall outside the scope of a general liability policy (depending on its terms) if it cannot be considered an occurrence or if it triggers an exclusion for intentional acts. Insurers have sometimes challenged intentional communications over texts or social media on these grounds. At the same time, an intentional act may form part of a larger constellation of actions taken by multiple actors, may involve negligent as well as

intentional conduct, and may produce unforeseen consequences for the recipient. In **State Farm Fire and Casualty Company v. Motta, 356 F.Supp.3d 457 (E.D. Penn. 2018),** the district court relied upon these factors and held that the insurer had a duty to defend a teenager accused of cyber bullying.

The district court described a pattern of cyber bullying and harassment of a high school girl, Julia Morath, by a classmate, Zach Trimbur, culminating in a vicious text message that prompted the school to suspend Mr. Trimbur when it was reported. He continued to harass Ms. Morath after his suspension, and she committed suicide the next day. Her parents filed suit against Mr. Trimbur and his parents, who made a claim under their homeowners' policy. State Farm provided a defense under a reservation of rights but filed a separate action seeking a declaration of no coverage because cyber bullying was "inherently non-accidental" and thus the injury could not have arisen from an occurrence.

The court rejected this claim. The court first acknowledged Pennsylvania cases holding that alleged faulty workmanship was not sufficiently "unexpected" to constitute an accident. **Kvaerner Metals Div. of Kvaerner U.S., Inc. v. Commercial Union Ins. Co., 908 A.2d 888 (Pa. 2006).** The court also recognized that allegations of bodily injury caused directly by "willful and malicious assault and beating" described an intentional tort rather than an accident. **Gene's Restaurant, Inc. v. Nationwide Ins. Co., 548 A.2d 246 (1988).** The court, however, distinguished these cases and their progeny on the basis of several factors. First, Pennsylvania tort law generally considers suicide to be an independent act not reasonably foreseeable by a tortfeasor, so Ms. Morath's suicide was at least potentially unexpected from the standpoint of Mr. Trimbur. Second, the lawsuit alleged a negligence claim against both Mr. Trimbur and his parents, and courts traditionally recognize a duty to defend when negligent conduct contributes to death at the hands of another person. Finally, the court emphasized that the duty to defend rested only upon the allegations of the compliant and the policy terms, not the underlying culpability or state of mind of Mr. Trimbur. The duty to indemnify, by contrast, might be very different once the underlying facts were established.

This case illustrates that even an undeniably intentional act, such as the transmission of an abusive and bullying text to a victim, may trigger a duty to defend when it forms part of a larger set of allegations involving negligence or unexpected consequences. Policyholders should therefore carefully consider whether other intentional acts or communications carried out over social media might also trigger a duty to defend under a general liability policy in light of the allegations as a whole and any unforeseeable actions taken by a third party.

Tech Risk Report

Protecting Innovative Companies Against 21st Century Risks

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Insurers Band Together To Certify Security Products

By Norton Cutler on May 13, 2019

In my previous blogs, I pointed out that security breaches are like death and taxes (i.e., unavoidable), and that insureds simply need a product that will pay for any losses from the inevitable security breaches. I also pointed out that insurance companies could help by certifying security products that were good enough to guarantee a payment under the companies' policies if there were a breach. The recent **Mondelez case** points out why insureds often wonder whether carriers really intend to pay claims. There, the maker of Oreo cookies bought a policy which covered intrusions into the company's computer code. After the advent of the Notpeya ransomware, the carrier refused claims valued in the millions based on the war exclusion. **See April 29, 2019 J. Davis post**. Relatedly, Merck reported $300m of losses from Notpeya, and insurer Hiscox reported that Cyber incidents rose from 45% to 61% of all companies surveyed between 2018 and 2019. **And the recent indictment** of two Chinese nationals for the Anthem hack that cost $115m also shows the likelihood of hacks and the resulting value of insurance that pays on such claims. **Law 360 May 9, 2019**. The option of buying a policy that would be guaranteed to pay as long as the insured purchased and properly used certified security software would go a long way toward increasing insureds' comfort that their cyber-related losses will actually be covered.

Such an option would be similar to the long-standing efforts of property carriers to inspect factories and other facilities and suggest safety improvements, or to the creation in the 1950s of the Highway Safety Institute to develop safer cars. As reflected in a Wall Street Journal **article** dated March 26, a group of insurers has announced a plan to certify providers of cyber security software under the name "Cyber Catalyst." It appears that Marsh will bring together a group of insurance companies such as Allianz, AXA, Munich, Zurich, and Beazley to jointly certify such software solutions. Marsh will not participate in the decision making, nor will Microsoft, which is serving as a technical advisor. Presumably, if an insured purchases cyber insurance from a carrier in this group as well as security software certified by the group, the carrier will not be able

to use an exclusion for not taking adequate precautions or any similar exclusion to bar coverage for a security breach.

The formation of this group may present antitrust issues, but as long as it acts in a non-discriminatory fashion, there should be a consumer benefit from having these certified solutions, which solutions should be found permissible. The group might also be able to improve the quality of the generally available security software by pointing out the weaknesses of submitted software. Because of the creation of an industry of security consultants who log into insureds websites and try to spot alleged security flaws and then either publicize those flaws or seek business to assist the software provider to remedy the issue, it will be interesting to see how the consultants interact with the group of insurers certifying software and the certified security software providers. The consultants may well disagree with the insurers, and it will be interesting to see if the insurers then side with the consultants or their certification decisions when adjusting claims.

Carriers may also offer premium discounts to insureds who buy the certified software, similar to safe driver discounts. As also mentioned **before in this blog**, many security software providers are now thinking about selling insurance for the inevitable breach as part of their products. This will raise its own regulatory issues about meeting the disparate rules of the fifty states about selling insurance, but it should provide a value-added product for insureds. Guaranteed coverage for a breach as long as the insured buys a certified security software system and uses it correctly may also provide other values to consumers. Given the arcane language used in many cyber policies, the security software providers might be able to persuade carriers to provide more understandable policies. Cyber Catalyst should also be able to assemble better data on security claims to give the companies more confidence in pricing their cyber policies, which should hopefully result in lower rates.

Security software providers may also consider seeking to persuade cyber carriers to accept the risk that, on occasion, utility may be more important than security. If the carriers certified products that allow use of password devices like facial recognition and fingerprints as opposed to requiring complicated computer-generated passwords or two-factor authentication that tend to complicate access to data and destroy utility, that might preserve ease of customers' access to their data. The goal should be to offer a product that provides compensation for the inevitable hack while still allowing a company to offer value to its customers by granting them relatively easy access to their own customer data or to on-line purchasing.

Carriers could also provide policies that pay claims when a security consultant or class-action lawyer claims to expose a problem that does not result in any loss of privacy or personal data, but leads to significant defense expenses. The recent case of ***USFI v. Xanitos*****, 19 CV 02947 (N.D.**

III), where the carrier is trying to avoid paying for defense of a suit alleging improper use of biometric software, shows how carriers might decrease use of effective biometric passwords by refusing to cover cases brought to enforce consent provisions, such as the one of Illinois biometric law at issue in *USFI*. This case admittedly involves a CGL policy, not a cyber policy, but if the carrier were to specifically approve the biometric software and defend it as part of a cyber policy, that would likely increase the usage of this feature, which makes it easier for employees to log into a job site containing sensitive health-care data.

Thus, it appears that the Cyber Catalyst project holds great promise for improving both cyber insurance and products that provide protection and compensation for the inevitable breaches that will continue to occur. Hopefully, it can also protect reasonable access to data and on-line transactions by counteracting the increasing trend of advocacy groups to limit use of, e.g., biometric devices based on their particular views of how to secure user privacy. These advocates seem to have encouraged various newspapers to run a campaign against their web based advertising competitors under the guise of protecting privacy. If successful, this approach may hamper ease of access to websites and decrease consumer utility. By providing reasonable insurance against such campaigns and lawsuits, the Cyber Catalyst project might well maintain ease of access and benefit the majority of consumers.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Biometrics Liability on the Rise: Are you Covered?

By Jim Davis on May 8, 2019

Biometric Privacy Lawsuits

In early 2019, the Illinois Supreme Court opened the floodgates for advancing private causes of action under the state's 2008 Biometric Information Privacy Act ("BIPA"), 740 ILCS 14 et seq. In ***Rosenbach v. Six Flags***, the Court found that no proof of actual injury or damage beyond technical infringement was necessary to state a claim under the BIPA. Now, Illinois courts are seeing a wave of BIPA class action lawsuits, even though the *Six Flags* case merely concluded that a biometric plaintiff had standing to sue and did not resolve the legal requirements necessary to prove a negligent or intentional violation of BIPA.

Currently, Illinois has the only biometric statute that provides for a private cause of action, but two other states have passed broad biometric privacy laws, including Texas (**Tex. Bus. & Com. Code Ann § 503.001** referred to as Texas Statute on the Capture or Use of Biometric Identifier) and **Washington (HB 1493** referred to as Washington Biometric Privacy Law). All of these privacy statutes codify the importance of properly handling, storing, and protecting biometric information, although they all define biometrics differently. The BIPA is arguably the most stringent in that it requires private entities that collect, capture, purchase, receive, or distribute biometrics (in most instances) to provide notice in writing and a obtain a written release. Many other states are contemplating sweeping privacy laws or have passed regulations governing particular biometric practices or products.

Coverage for Biometrics

As expected, coverage disputes relating to BIPA class actions are emerging. Allegations in underlying class actions and coverage provisions in policies can vary widely. Many complaints include claims outside of the BIPA, such as common law causes of action for negligence or breach of privacy, or assertions of security breaches and accidental releases of biometric

information. Many policies contain a duty to defend the entire claim if there is a potential for coverage as to any part of the case.

These BIPA lawsuits may implicate a broad range of insurance policies, including the following:

Cyber Liability coverage is often available depending on the actual provisions of the policy, which vary significantly and are often negotiable. Policyholders should pay attention to the types of events that trigger coverage and to the definition of personally identifiable information. Allegations of a security breach may separately implicate coverage.

General Liability policies may respond under the personal and advertising coverage subject to various exclusions. Limited cyber coverage also may be available to expand the definition of personal and advertising coverage, including by endorsement.

Employment Practices Liability coverage may be available to the extent the purported class action involves the gathering of biometrics in the course of employment.

Media Liability coverage often includes coverage for certain privacy violations and may be incorporated into another type of policy.

Conclusion

The extent of liability for BIPA violations is still in flux in Illinois, but plaintiffs are seeking enormous damages in large class actions. Statutory regulation of biometrics throughout the country is on the rise and other states may soon follow Illinois in allowing private causes of action. Given these realities, companies in the biometrics business should carefully review their insurance program now to avoid any gaps in coverage.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Collateral Damage: War Exclusions and Cyber Coverage

By Jim Davis on April 29, 2019

The entire insurance industry is suddenly abuzz about the rarely discussed “war exclusion.” A standard provision in most policies that excludes claims caused by a hostile or warlike action in time of peace or war, usually by a military or a government/sovereign power, is all the rage. Why? The billions of dollars of damages caused by the NotPetya virus and insurers attempts to avoid paying them.

The NotPetya virus was released in 2017 apparently to attack accounting software in Ukraine, perhaps as an attempt to disrupt Ukraine’s supply network, but it quickly spread and caused collateral damage to a multitude of policyholders around the world. At first, insurers believed it was a criminal ransomware money making exercise, just like the Petya ransomware attacks in 2016. Now, insurers insist it was an act of war, because the virus looked like ransomware, but ultimately caused only destruction. The US and UK believe the Russian government or military was “almost certainly” behind the attack. Russia denies any involvement and points out that the virus spread to Russian commercial systems as well. No indictments have been filed and public information on the source of the attack is limited.

Not surprisingly given the stakes, coverage litigation over denials under the war exclusion for the NotPetya virus are brewing. A late 2018 lawsuit filed in Chicago revealed that Zurich was denying coverage under a property policy based on a “war exclusion” for $100 million in damages caused by the NotPetya virus. The policyholder, Mondelez International, maker of various essential food items, including Oreo cookies and Toblerone chocolate, did not realize it was at war with anyone when the virus wiped out thousands of its servers and laptops in June 2017. Likewise, it was recently reported that international law firm DLA Piper is apparently moving to sue Hiscox for coverage after a war exclusion denial. The law firm’s computer systems were badly impaired by the virus and allegedly required 15,000 hours of IT overtime to get back up and running.

The use of the war exclusion here seems quixotic and beyond the expectations of ordinary policyholders when purchasing their insurance program. Even brokers are dismayed and are openly discussing war exclusion denials as overreach (see “NotPetya Was Not a Cyber ‘War’” Marsh & McLennan Insights **http://www.mmc.com/insights/publications/2018/aug/notpetya-was-not-cyber-war.html**). In most instances, insurers will bear the burden of proving that these circumstances fall under the war exclusion. As noted above, proving that the virus was released by a state actor as part of a hostile or warlike action is a serious hurdle.

Meanwhile, policyholders need to pay attention when renewing their insurance programs to make sure they are getting coverage for these potential cyber risks. The insurance industry is scrambling to change language in policies, so they do not have to prove up the requirements of the traditional war exclusion. Policyholders can expect to see the introduction of broader exclusions in non-cyber policies, such as general liability and first-party property policies. On the other hand, many cyber insurers may be willing to provide explicit cover for these types of claims or, at a minimum, negotiate a narrower war exclusion. Change is afoot!

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

How Risky is the Insurance from a Non-Admitted Insurer?

By Jay Rossiter on April 17, 2019

Should you stress if the insurance company issuing the policy that is supposed to be protecting your business—whether in a certificate of insurance you received from a third party or within your own insurance portfolio—is "non-admitted"? As discussed below, there is no need to sweat.

An "admitted" insurance company is one that has been approved by a state's department of insurance. This generally means that the insurance company must file policy forms, underwriting guidelines, and rates with the state for approval. Admitted insurers also pay into state guaranty funds, which are designed to step in if the insurer becomes insolvent. Non-admitted insurers, also called surplus lines insurance, are not subject to those same regulations.

At first blush, it would seem more prudent to have an insurance company backed by the state insurance commissioner, particularly if the insurance company goes out of business. But, the truth is that non-admitted/surplus lines insurance is subject to other regulations and can actually be better suited to address some of the unique risks for tech and other companies that are trying to implement creative innovations to disrupt the marketplace.

Generally, surplus lines insurance is sold through surplus lines brokers, who themselves are regulated by each state. In most states, qualified brokers are required to demonstrate that they attempted in good faith to place insurance with an admitted carrier before going the non-admitted route. Why would an admitted insurer decline to insure a particular risk? For lots of legitimate reasons. Typical risks underwritten by the surplus lines market fall into three basic categories: (a) non-standard risks that do not have typical underwriting characteristics, (b) unique risks that are not addressed by standard policy forms, and (c) higher-than-normal coverage limit requirements, where a business seeks more coverage than insurers are willing to provide.

Business insurance for contractors in New York City, for example, is sometimes unavailable because some underwriters find certain operations in that market too risky. Similarly, businesses

along the Gulf Coast may not find property insurance from admitted insurers. The same might be said for emerging technologies for which insurers do not have a lot of past experience.

Is the insurance itself unreliable, particularly if there is no state guaranty fund? Statistics from the credit rating firm A.M. Best show that the record of insolvency for surplus lines is roughly equivalent to that for the admitted marketplace. If your broker is unable to place insurance with an admitted insurer, obtaining coverage from a non-admitted insurer might not be a bad thing (although it might cost you more). Rather than a one-size-fits-all policy form, surplus lines can offer more flexibility for new products and innovations. Standard market forms might suit certain risks just fine. But they might also be completely inadequate to unique business models or risks, whether driven by tech advances or by something as simple as a geographic focus that is unfamiliar to admitted carriers, or one they are not used to underwriting (e.g., no loss history based on similar past claims).

Some suggestions: for your own insurance needs, retain a skilled broker with experience handling businesses and technologies as innovative as your own. Such a broker is likely to be in the best position to track down the types and levels of insurance that best fit your business profile. This may or may not include surplus lines. If your business model is unique enough, coverage from a non-admitted insurer may be appropriate. Coverage counsel can also advise you about whether the insurance proposed by your broker (or in a certificate of insurance) properly takes your business and risks into account.

Many businesses protect themselves by requiring vendors and other third parties with whom they are doing business to expressly indemnify them and add them as additional insureds under the third party's insurance.

Check the ratings of the insurance company providing insurance to you or to the third party supplying you with a certificate of insurance

You can protect your business by insisting in your agreements on minimum ratings for the insurance that a third party is required to have (for example, A+) and requiring in advance copies of (a) relevant certificates of insurance and (b) the policy language or endorsement that makes you an additional insured; and—if you really want to protect yourself—reserving for yourself the right to inspect the third party's insurance policies, so that you can verify the coverage language and double-check the credit ratings of the insurance companies proposed.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Beyond GDPR: Insurance Coverage for Emerging Cybersecurity and Privacy Regulatory Exposure

By Freya K. Bowen on April 10, 2019

The European Union's sweeping Global Data Protection Regulation (GDPR), which took effect on May 25, 2018, dramatically expanded the compliance obligations of companies collecting or using European Union citizens' personal information. It also substantially increased regulatory exposure for companies due to its strict requirements and draconian penalties for non-compliance, including potential fines of greater than 20 million Euros or 4% of a company's annual worldwide revenue. **GDPR Art. 83, § 5.** See Perkins Coie's **GDPR Resources** for an overview of the regulation, and **Will Your Cyber Policy Provide Coverage for GDPR Violations?** for a discussion of insurance coverage issues arising from the regulation. Yet the new regulatory landscape facing companies that collect, use, or manage consumers' personal information has expanded far beyond the GDPR, and many United States jurisdictions have enacted or are in the process of enacting regulations governing the collection, storage, and use of consumer information. As a result, any company that handles consumer personal information must have a thorough understanding of these regulations and must make sure that its insurance program aligns with its regulatory exposure in order to effectively manage the risks arising out of burgeoning cybersecurity and privacy regulations.

One of the most prominent recently enacted cybersecurity and data protection law is **California's Consumer Privacy Act of 2018 (CCPA)**, sometimes dubbed "the US GDPR," which will take effect on January 1, 2020. A company need not have a brick-and-mortar presence in California to be subject to the CCPA: for-profit companies that collect and control personal information of California residents must meet the CCPA's requirements if they (1) have annual gross revenues in excess of $25 million; (2) receive or disclose the personal information of 50,000 or more California residents; or (3) derive 50 percent or more of their gross annual revenue from selling the personal information of California residents. The CCPA also applies to corporate affiliates of these businesses that share their branding. As a result, many companies across the country and

even outside the United States who count California residents among their customers will be subject to the CCPA.

The CCPA provides consumers with specific rights and choices concerning the use of their information and requires businesses to provide notices and disclosures to consumers in various circumstances. For instance, businesses must disclose to consumers, at or before the point of collection, the categories of personal information to be collected and the purposes for which the information will be used. Businesses must also notify consumers that they have the right to opt out of the sale of their personal information. Upon customer request, a business must disclose what information it has collected about the consumer, the sources of this information, the business purpose for the collection, and any third parties to whom the information has been sold. Businesses must also delete information collected about a consumer when requested, and direct service providers to delete that customer's information as well. Businesses in violation of the CCPA are subject to a remedial injunction and penalties of up to $2,500 per violation, and $7,500 for each intentional violation. Notably, in addition to these penalties, the CCPA also gives consumers a private right of action for data breaches arising from "a violation of the duty to implement and maintain reasonable security procedures and practices."

Other states have also enacted legislation protecting the personal information of their residents. For example, Massachusetts has **enacted amendments**, effective April 11, 2019, to its already comprehensive data protection and privacy law — **201 C.M.R. 17**, Standards for the Protection of Personal Information of Massachusetts Residents, or "Massachusetts Standards." The Standards provide robust data-security-program and encryption requirements, including the obligation to contractually bind a business's third-party service providers to meet the Standards. Penalties include injunctive relief and fines up to $5,000 per violation, and violators will incur the costs of investigation and litigation. The Standards also require that, in the event of a data breach, companies must provide specific details to the state attorney general and the Office of Consumer Affairs and Business Regulation. If individuals' Social Security numbers are disclosed, the company must offer credit monitoring services at no cost for 18 months. The amendments expressly prohibit delaying notice in order to determine the number of individuals affected, requiring instead that notices be sent out on a rolling basis.

Colorado likewise strengthened its consumer data protection law with **amendments** that went into effect on September 1, 2018. The new amendments require businesses that collect personal information of Colorado residents to "implement and maintain reasonable security procedures and practices," and to contractually require service providers to do the same. Businesses must also develop written policies for the destruction or disposal of personal information once it is "no longer needed." The amendments impose stringent data-breach-notification obligations: notice

letters to Colorado residents must contain specified details, and companies must notify the state attorney general if notice of a security breach is given to 500 or more Colorado residents. Colorado also joins **Florida** as the only other state to require notification of a security breach within 30 days.

Cybersecurity regulations specific to particular industries have also recently been enacted in many states. For instance, New York's comprehensive cybersecurity regulations for financial institutions, **NY CYCRR 500** went into full effect on March 1, 2019, after phased implementation. The law requires financial institutions to designate a "Chief Information Security Officer," to implement a cybersecurity policy, to provide an annual cybersecurity report to the institution's full board of directors, and to monitor third-party service providers under quite stringent standards. **Vermont's new law** requires "data brokers" to implement specific security measures and to register with and provide certain disclosures to the state attorney general as of January 1, 2019. After the National Association of Insurance Commissioners (NAIC) promulgated a model **cybersecurity regulation** for insurance carriers in 2017, **South Carolina**, **Ohio**, and **Michigan** all adopted the law in 2018.

Given the rapidly expanding universe of cybersecurity regulations and the extra-territorial reach of the GDPR and many state regulations, businesses should regularly re-assess their cybersecurity insurance programs to make sure they are adequately covered in the event of regulatory actions. Below is a non-exhaustive list of issues to consider when analyzing a company's coverage for regulatory risk:

Policy Definitions vs. Regulatory Definitions: Many state regulations define key terms such as "personal information" or "personal data," "data breach," and "security event," which are typically also defined in cybersecurity policies. A cyber policy definition that is narrower than a regulator's definition of a term could leave a policyholder exposed in the event of regulatory action, or, at minimum, could introduce ambiguity and potentially costly uncertainty into coverage questions. The policy definition of "regulatory action" should also encompass the various actions pertinent regulators are empowered to take, such as seeking injunctive relief or ordering particular remediation efforts.

Insurability of Fines and Penalties: Many European Union countries and a number of United States jurisdictions prohibit insurance coverage for fines and penalties. The jurisdiction specified in any choice of law provision in the policy should permit coverage for fines and penalties. In addition, policyholders should look carefully at any provision specifying that penalties are covered "as allowed by law" in order to foreclose the argument that insurability is determined by the law of the jurisdiction imposing the penalty, rather than the jurisdiction governing the policy. Ideally, the

policy should clearly provide that fines and penalties are covered to the fullest extent possible under the law of the most favorable jurisdiction.

Coverage for Non-Penalty Expenses: Regulatory risk encompasses more than just fines and penalties and may not necessarily arise in connection with a data breach. Many regulators are empowered to seek injunctive relief, forcing a business to take specific actions in order to come into compliance with the regulations. Policyholders should make sure that their cyber policies do not limit regulatory coverage when the pertinent regulators take action without an actual breach. Policyholders should also look closely at the policy definitions of “claims expenses,” “damages,” and “loss” to make sure they are broad enough to encompass the costs associated with regulatory action, such as investigation costs, remediation costs (for instance, providing free credit monitoring when required), and compliance with notice requirements.

Intentional Acts Exclusions: Cyber policies may contain exclusions for intentional acts. These exclusions are particularly problematic with respect to regulatory coverage, as some regulations, such as the CCPA, impose heightened penalties for “intentional” violations of the regulations. While the conduct necessary for a regulator to find intentional conduct may differ from the traditional understanding of the term in the insurance context, the presence of this exclusion potentially leaves cyber policyholders exposed.

Imputation Provisions: Policyholders should also look carefully to see whose conduct can be imputed to the policyholder. For instance, actions by a rogue employee who deliberately sabotages an organization’s cybersecurity or misuses consumers’ personal information may create liability for the organization under a respondeat superior theory or even potentially give rise to a regulatory finding of “intentional violation” of cybersecurity regulations. Ideally cybersecurity policies would have a strong non-imputation provision strictly limiting whose acts can be imputed to the company for coverage purposes.

As more United States and foreign jurisdictions adopt and expand regulations governing cybersecurity and data privacy, and as cyber insurance claims arising out of regulatory enforcement actions are assessed and resolved or adjudicated, new trends and issues are bound to arise. Companies handling personal consumer information should continue to monitor their expanding regulatory exposure and reassess their cyber insurance program in light of these developing trends in order to manage their regulatory risk.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Companies Engaged with Digital Assets Should Push For D&O Coverage That Protects Traditional Securities Activities

By Robert P. Jacobs on March 26, 2019

Companies engaged with digital assets, particularly those companies without a track record, are finding it to be a struggle to procure broad directors & officers ("D&O") liability coverage. Specifically, insurance underwriters are spooked by the regulatory uncertainty surrounding digital assets, particularly Initial Coin Offerings ("ICOs"), which have emerged as an alternative to traditional equity offerings, *e.g.*, the sale of stock in a venture. The reality, however, is that many companies engaged with "coins" or "tokens" or other digital assets also raise capital through traditional securities offerings, and they need protection for those activities. But many underwriters are not willing to sell coverage for those traditional activities, merely because the company also is engaged in the digital asset space.

Indeed, mainstream companies that wished to raise funds from the public would begin to do so by selling shares through an Initial Public Offering ("IPO"). In the cryptocurrency world, the ICO is the rough equivalent to the mainstream IPO. Although there has been some debate as to whether the term "Initial Coin Offering" is a misnomer, suffice it to say that, by and large, the "offering" is used as a way to raise money by selling "coins" or "tokens" to investors that want to have a stake in the enterprise, whether it be a new type of cryptocurrency, an app, or some other related service, such as an exchange for trading cryptocurrencies.

Over the past several years, the use of ICOs has increased dramatically, from less than 10 in 2014 to more than 600 in 2018. The increase in ICOs has raised concerns among regulators, who feared that the ICOs could be used to take advantage of an unwary or uniformed public. One of the earliest regulators to get involved was the Financial Crimes Enforcement Network (FinCEN), which became concerned about, among other things, whether the cryptocurrencies were being used for money laundering and thus violated the Bank Secrecy Act. In 2015, the Commodity Futures Trading Commission (CFTC) determined that cryptocurrencies—possibly

including digital tokens sold through ICOs—were commodities, and therefore sought to regulate them as such.

But perhaps the most dominant question as of late is whether coins or tokens sold through ICOs constitute the sale of securities. Accordingly, in 2017 the Securities and Exchange Commission (SEC) entered the fray issuing what has become known as its "**DAO Report**," which investigated whether tokens issued by "The DAO"—an acronym for Decentralized Autonomous Organization—were securities. The SEC described the DAO as a "for-profit entity that would create and hold a corpus of assets through the sale of DAO Tokens to investors, which assets would then be used to fund 'projects.'" The SEC continued by explaining that the "holders of DAO Tokens stood to share in the anticipated earnings from these projects as a return on their investments in DAO Tokens." Ultimately, the SEC concluded that DAO Tokens were securities under the Securities Act of 1933 and the Securities and Exchange Act of 1934. From this, the SEC advised all entities that use distributed ledger or blockchain-enabled means for raising capital to ensure compliance with federal securities laws.

Even with this guidance, there is still a general sense in the insurance industry that companies that deal in any way with "coins" or "tokens" are not good risks. This may stem from the belief that many ICOs still do not comply with securities laws and, therefore, do not provide protections to investors. Insurance underwriters also seem wary that ICOs are still a means to fraud, money laundering, and other illicit activity.

So what this means is the following: companies that are in any way engaged with tokens or digital coins are finding it to exceedingly difficult to procure D&O coverage that provides protection for any liabilities arising out of ***any*** securities activities, even in traditional activities such as offering shares to accredited investors or otherwise. This is true even if a company does not issue a coin or token for the purposes of fundraising at all. For example, a company may raise all of its capital through traditional means, while issuing tokens or coins for some other purpose, such as as tickets to concerts or sporting events. Some companies may issue tokens or coins that can be used to buy something at a discount that will be released in the future, such as a case of reserve wine.

Specifically, when faced with a company that in any way handles digital coins or tokens, some insurers are insisting on what they call a "Full Securities Activities Exclusion," which, as its name implies, is very broad and purports to bar coverage for such things as "any allegation that any prospectus, interim statement or public announcement…contains an untrue statement of material fact, or…omits a material fact…," among other things. At the same time, insurers are also seeking to tack on a "Full Coin Offering Exclusion," which is meant to bar coverage for any liability

“based upon, arising out of, directly or indirectly resulting from or in any way involving a Coin Offering” which, in turn, is defined as, in general, “an actual sale of tokens by the company” to the public.

If it is the regulatory uncertainty surrounding digital coins and tokens, and/or any perceived prospects of fraud, etc., which are making insurers uneasy, they should focus on that, and not broadly bar coverage for traditional securities activities. Companies engaged with blockchain technology, cryptocurrencies, and other digital assets that also raise capital through traditional means, should make sure that the insurers from whom they are hoping to procure coverage understand this distinction. This probably will require teaming up knowledgeable brokers with the transactional and regulatory attorneys that provide advice and counsel to the company, and making a presentation to the insurance underwriters so that they can fully understand the business and feel secure that the company is acting responsibly and seeking to be compliant. Protection for securities activities is important for any company that hopes to grow and thrive, and time should be taken to make sure that insurance underwriters do not have knee-jerk reactions as soon as they hear of digital assets.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Social Media and New Businesses: Can Anticipatory Use of Social Media Threaten Insurance Coverage?

By Jeff Bowen on March 19, 2019

Many businesses rely upon social media to raise awareness and enhance visibility of a new product or new line of business. Social media platforms such as Facebook are often used to generate buzz around an opening or a launch before it takes place. Anticipatory use of social media, however, can complicate insurance coverage if the right policies are not already in place. The Idaho Supreme Court recently upheld the denial of coverage to a business that had published a preview of a new logo prior to opening. ***Scout, LLC v. Truck Ins. Exch.***, 434 P.3d 197 (2019). The court held that a Facebook post by the insured pub showing a close facsimile of the anticipated logo constituted a "prior publication," triggering an exclusion under the pub's subsequently purchased commercial general liability policy. Although some other courts have reached different conclusions in relatively similar circumstances, the case stands as a cautionary tale for new businesses.

The plaintiff in *Scout* had purchased a restaurant in downtown Boise and planned to renovate and reopen the space as the Gone Rogue Pub. Shortly after purchase, Scout posted a picture of the planned logo on its Facebook page and registered the name with the Idaho Secretary of State. Prior to opening, no other advertising or publication used the logo. The following month, Scout purchased commercial general liability insurance, obtained the requisite licenses, and opened the pub. About two months later, the Oregon Brewing Company objected that the Gone Rogue logo and related merchandise violated its federally registered trademarks. When negotiations over licensing proved unsuccessful, OBC filed suit, alleging trademark infringement, unfair competition, Lanham Act violations, and similar claims. Scout notified its insurer, who acknowledged that the complaint alleged advertising injury under the policy but declined to defend on the basis of an exclusion for "material whose first publication took place before the beginning of the policy period." Scout then settled with OBC and sued the insurer.

The district court dismissed the lawsuit, and the state supreme court affirmed, rejecting a series of arguments that any new business might make in Scout's position. First, applying Idaho law, the court declined to force the insurer to consider facts outside the complaint, such as when the business had opened (though the court also held that that wouldn't have changed the result).

More importantly, the court found that the exclusion unambiguously precluded coverage for *any* prior publication, regardless of whether that publication had been injurious to the claimant. The court distinguished a Seventh Circuit case which had reached the opposite conclusion when interpreting a similar exclusion. ***Capitol Indem. Corp. v. Elston Self Service Wholesale Groceries, Inc.***, 559 F.3d 616 (7th Cir. 2009). In *Elston*, a distributor had sold Newport cigarettes for some time and then began selling counterfeit cigarettes in the same Newport packaging. The Seventh Circuit held that the exclusion only applied to "prior publication of the same actionable, injurious material alleged in the underlying complaint." Because the prior "publication" involving legitimate cigarettes was not actionable, the exclusion did not apply. The Idaho court rejected this approach, holding instead that the "relevant question is not when the claim first became actionable, but when the material giving rise to the claims was first published." 437 P.3d at 205 (quoting ***Matagorda Ventures, Inc. v. Travelers Lloyds Ins. Co.***, 203 F.Supp.2d 704 (S.D. Tex. 2000)). Thus, the Facebook preview of the new logo was sufficient to trigger the exclusion and preclude coverage, regardless of whether the Facebook post in itself could have given rise to a claim.

Finally, Scout argued that, even if the Facebook posting constituted a prior publication, the complaint alleged separate violations committed *after* the policy period began that independently triggered coverage. For example, the complaint alleged placement of the infringing logo on glassware as well as "cybersquatting" through a new website, neither of which happened before the business opened. The court acknowledged that a duty to defend might arise despite a prior publication if a complaint also alleged sufficiently independent "fresh wrongs."

The Idaho court, however, declined to apply the "fresh wrongs" doctrine, citing instead ***Street Surfing, LLC v. Great American E & S Ins. Co.***, 776 F.3d 603 (9th Cir. 2014), and ***Hanover Ins. Co. v. Urban Outfitters, Inc.***, 806 F.3d 761 (3rd Cir. 2015). In *Street Surfing*, the policyholder allegedly violated trademarks with respect to skateboards before the policy period and with respect to skateboard accessories after the policy period. The court concluded the alleged wrongs were substantially similar, noting that "if Street Surfing's post-coverage publications were wrongful, that would be so for the same reason its pre-coverage advertisement was allegedly wrongful: they used Noll's advertising idea in an advertisement." 776 F.3d at 614. Similarly, the *Hanover* court declined to find "fresh wrongs" in a series of alleged trademark infringements by Urban Outfitters relating to the Navajo name and trademark. The Idaho court likewise concluded

that, despite the presence of new claims after the policy period began, the complaint alleged a "constant agglomeration of continuing harm stemming from the use of the ROGUE mark." 434 P.3d at 208.

As this case illustrates, anyone seeking to generate buzz around a new business through social media should consider the risk of an advertising injury claim and whether appropriate liability insurance has been secured.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Meeting the Terms of the Exceptions in Your Cyber Policy

By Norton Cutler on March 5, 2019

In my last posting on this blog, I opined that cyber incursions and the resulting lawsuits, defense costs, and damages payments are as inevitable as death and taxes. Thus, most companies are now trying to purchase some type of cyber insurance to cover these risks. The next question is whether your insurance will really cover a particular risk you face. My last article discussed a single product that would provide security and guarantee coverage for any breach up to a specified limit.

Today I want to discuss other defensive measures that a company might take against the inevitable, and how that might make coverage in the event of a breach more likely under a standard cyber insurance policy. Our last posting by Ms. Del Prete discussed the standard exclusions and conditions in the most common cyber policies. Those policy provisions require, e.g., that the insured follow industry standard security practices and take reasonable precautions against data breaches before coverage will attach for an incursion. Subject to the purchase of an extended retroactive date, they also exclude breaches that occurred long before the beginning of the policy or which were facilitated by an incursion that occurred prior to the beginning of the policy.

Of course, these provisions raise additional questions, such as what are industry standard security practices or reasonable precautions? There seem to be no decided cases on these issues yet. But all sorts of security packages that might meet these standards are commercially available, and some new products may provide interesting adjuncts to existing cyber defenses. These new products typically monitor all data traffic to and from a company's system to identify attempted attacks or phishing to facilitate a future attack, system vulnerabilities, and outside access to websites and countries that suggest that someone may be placing a company's system in danger. For example, if an employee who has no need to deal with countries like China, Russia, or various eastern European nations, which are generally considered hotbeds of hacking, starts contacting websites in these countries, then the software will question that access and

notify the company, so that the company can eventually cut off the link if there is no good explanation given. If hackers attempt to breach a firewall or otherwise enter a computer or system to explore future attack possibilities, an alert is given to shut down that user or analyze the specific attack or phishing. The targeted alerts provided by these new products may make it easier to resolve more important issues and ignore other less important ones. Such services may also help detect and log efforts to find a breach as soon as or even before it happens, so as to avoid policy exclusions for losses due to prior acts and for breaches that occurred prior to the effective date of the policy (or the retroactive date).

It appears that these types of new products and services may be folded into network equipment or services provided by ISPs as standard security defenses. If a purchaser of cyber insurance does not also purchase these services, that may allow the insurer to seek to decline coverage for a subsequent breach. Indeed, perhaps the carriers themselves will provide and/or certify such adjunct services (as some carriers have already done), much as they have also provided safety inspections and other loss-prevention services as part of their standard property and casualty insurance services. The broad use of such products and services ultimately may even lower their cost and make them even more desirable. It could certainly make them a required part of security defenses that insurers may require policyholders to implement to avoid policy exclusions.

The anticipated requirement for such products and services also presents the question whether they may make the policyholder's website or other business less user friendly by requiring more password-type defenses before a customer can access her own data or otherwise use the site. It appears that using facial recognition and/or fingerprints as a permitted substitute for increasingly bizarre passwords and two-factor authentication, both of which make it hard for a customer to access her data, might well solve that issue. These types of alternative authentication would appear to provide relatively hack-proof identifiers for customers seeking to access their data on a site.

Unfortunately, recent regulatory efforts in Illinois and California seem to detract from making data access more user friendly by requiring increasing levels of specific consent for storing of the data required for use of this type of fingerprint or facial-recognition authentication. While it is an issue whether third parties might misuse both types of data if they can gain access to it, the government has had a treasure trove of fingerprint data for a very long time, and it seems that facial data is no more subject to abuse. There is also a claim that faces and fingerprints can be spoofed, but they still seem more hack-proof than random passwords and two-factor authentication.

Regardless, a carrier might well require that its insureds use facial recognition and fingerprints as a permitted substitute for passwords, with proper customer consent, as an alternate reasonable method of establishing precautions against an incursion. Much as insurance carriers helped establish safety practices in factories and other brick-and-mortar industries, they can assist here to set baselines for proper security practices like passwords, facial recognition, and fingerprints; and in the process, they may be able to lower the cost of obtaining those protections as they spread across the web.

Some incursions may cause little or no real harm, but the litigation and resulting mitigation can consume significant resources, and setting well established baselines for reasonable efforts to prevent incursions would at least lower the cost of such litigation. This might in turn decrease the cost of obtaining cyber insurance as carrier payouts should decrease and the cost of the security software might also go down.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Common Exclusions Invoked by Cyber Carriers to Deny Coverage

By Catherine Del Prete on February 20, 2019

Often called the "wild west," the cyber insurance marketplace offers a wide variety of policy forms that vary drastically in the scope of coverage provided. This is further compounded by the relatively small amount of case law analyzing cyber policies and the quickly-evolving cyber risks that companies face. Insurers are quick to deny coverage based on the many exclusions in cyber policies, often leaving policyholders with the option of either spending money to fight their insurer in court or accepting the carrier's denial. If your company is insured by a cyber policy (or, for that matter, any type of an insurance policy), you should carefully review the policy, understand its exclusions, and, where possible, take steps to implement practices and procedures to ensure that your company's activities do not fall within the enumerated exclusions. Cyber insurers are often willing to modify exclusions in cyber policies to carve back certain coverages, but only when asked to do so. Analyzing the policy and negotiating with the carrier on the front end, before a claim occurs, can save your company both time and money on the back end if a claim arises. Below, we discuss some of the more frequently-invoked cyber policy exclusions that carriers use to deny coverage.

- **Security Standards Exclusions**: Some cyber policies exclude coverage for claims based upon the insured's failure to maintain minimum security standards. The phrasing of these exclusions varies widely. Some policies exclude coverage for an insured's failure to comply with "industry standards," while other policies contain endorsements specifically listing "Minimum Required Practices" that the insured must follow. Another iteration of this exclusion ties the insured's obligations to the security procedures identified in their cyber insurance application. Other policies contain hybrid exclusions that combine various portions of the above. Depending on how it is written, this exclusion could potentially preclude coverage for almost every data breach. Policyholders should be careful to accurately complete cyber insurance applications and to confirm that security protocols identified in the applications are in place for the duration of the policy period. Further, if your

company's policy has an iteration of this exclusion, you should request that it be removed or, alternatively, that any ambiguities (like a requirement of compliance with the vague and undefined term "industry standards") be clarified by the carrier in an endorsement.

- **Bodily Injury and Property Damage**: Most cyber policies exclude coverage for claims arising out of "bodily injury" and "property damage." More and more frequently, general liability policies (which would normally provide coverage for these types of claims) also contain exclusions that may apply to certain cyber-related incidents. *See, e.g.*, **Insurance Services Office, Inc., Exclusion for Access or Disclosure of Confidential or Personal Information and Data-Related Liability (Form No. CG 21 07 05 14)**. If a cyber incident at your company could result in bodily injury or property damage, you should ensure that your company's insurance portfolio contains the appropriate coverages so you are not left uninsured in the event of a claim. In addition, companies should look carefully at the definition of bodily injury in their cyber policies to confirm that coverage for claims of mental anguish, mental injury, shock, emotional distress, and humiliation are carved back, as plaintiffs almost always cite these injuries as damages stemming from a data breach.
- **War, Terrorism, Invasion, or Insurrection**: Almost all cyber policies exclude coverage for loss from acts of war, terrorism, invasion, and/or insurrection. The exclusions are often written expansively and, given the proliferation of state-sponsored, political, and ideological cyber attacks, could preclude coverage for most security breaches. Many insurers are willing to modify these exclusions to carve out coverage for "cyberterrorism" or "electronic terrorism."
- **Prior Acts**: Cyber policies, like almost all insurance policies, exclude coverage for claims based upon wrongful acts that occurred before a certain date (often called the "Retroactive Date"). The Retroactive Date is often the first date that an insurer issued a policy to the insured, meaning that this exclusion is usually not an issue for companies that have renewed their insurance policy with the same carrier for extended periods of time. However, this can create significant issues for companies switching cyber insurers or companies that were previously uninsured in the cyber realm. Cyber breaches can take place over long periods of time and are often discovered by companies long after the breach occurred. Cyber policies are "claims made and reported" policies, meaning that they will only respond to claims that are made against or discovered by an insured during the policy period. This also means that an insured must provide notice of the claim to its cyber insurer during the policy period for coverage to exist. If you submit a claim under a cyber policy that arises from a breach that occurred prior to the Retroactive Date, your company may be left uninsured for a claim. Companies should be aware of this limitation on coverage. Before changing your cyber carrier, be sure to purchase an extended discovery period, which

provides an additional period to report claims that would have been covered by the non-renewed policy. Alternatively, consider obtaining a Retroactive Date that predates the inception of your new policy.

- **PCI Fines & Assessments**: Almost all cyber policies contain contractual liability exclusions, some of which have been interpreted to exclude coverage for PCI fines and assessments. *See, e.g.*, ***P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*****, CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016)**. Other cyber policies expressly exclude coverage for PCI fines and assessments. If your company could be subjected to PCI fines and assessments following a breach, you should carefully review your cyber policy to make sure that it expressly provides coverage for them.
- **Laptop Exclusion**: Depending on your cyber policy's exclusions, your company may not be covered for claims based upon an employee's lost company laptop or other portable electronic device. Some insurers are willing to remove this exclusion altogether. Other carriers may be willing to modify the exclusion to only apply to claims arising from the loss of an *unencrypted* portable device.

Of course, the above list is not meant to be exhaustive, but is instead intended to be used as a starting point to identify some frequently raised cyber coverage exclusions. Risk managers and cybersecurity personnel should critically evaluate the coverage and exclusions within a company's cyber insurance policy to ensure that there are no unintended gaps.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Protecting your Website with an EPL Insurance Policy

By Jay Rossiter on February 14, 2019

Title III of the Americans with Disabilities Act (ADA) provides that

> No individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation.

42 U.S.C. Section 12182(a). What about a website? Is that a "place of public accommodation"? The answer to that question could make a big difference in determining whether your business faces legal risks and whether you can protect against those risks with insurance. A recent decision out of the Ninth Circuit highlights the split in United States jurisdictions about whether a website is subject to the prohibitions against discrimination found in the ADA.

On January 15, 2019, the Ninth Circuit confirmed that the online ordering feature offered by Domino's Pizza was subject to the protections afforded under the ADA. *Robles v. Domino's Pizza, LLC*, **913 F.3d 898 (9th Cir., Jan. 15, 2019)**. There, a blind man was unable to order pizza from Domino's, even with the screen-reading software he was using. The court held that the Domino's physical restaurants are places of public accommodation, and that since customers use the website and app to locate nearby Domino's restaurants for at home delivery or in-store pickup, the website was subject to the ADA as well—it was the nexus between the website and the physical restaurant that brought the website within the requirements of the ADA.

What if your business operates a website or app without a "physical" storefront? In the Ninth Circuit, the courts have held that the ADA does not apply.

But, be aware that the rule is different in the First and Seventh Circuits, where the courts have rejected the proposition that a website cannot be a public accommodation without a nexus to a

physical place. There, web-based services alone can be the subject of a Title III discrimination action.

Clearly, if your business has a physical location that customers can visit, it must comply with the ADA and is at risk for a discrimination claim if it fails to do so. But, if you plan to do business in some states—like Illinois, Massachusetts, or Wisconsin—you are at risk even if you don't have a physical location. This is where the right type of Employment Practices Liability (EPL) insurance can help. EPL policies cover claims by employees, but also can cover discrimination claims by third parties. Make sure you have that coverage when you are purchasing or renewing your EPL policy, and check for it immediately if you are threatened with a lawsuit.

ADA and other discrimination claims by consumers are frequently brought in class action form, which can be costly and time-consuming to defend. Your EPL insurance can help mitigate those costs. Although ADA lawsuits frequently request injunctive relief involving, e.g., making changes to a facility or website, which many EPL policies will not cover the costs, the costs of defending a class action claim are covered and, depending on your policy, so might be the costs of paying for the other side's attorneys' fees. Note also that ADA claims are often coupled with other causes of action, like alleged violations of the Unruh Civil Rights Act **(Cal. Civ. Code § 51. et seq.)** or the Calif. Disabled Persons Act **(Cal. Civ. Code §§ 54-54.3)**, which may seek damages that are covered by your EPL policy.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Recent Developments in Yahoo and Equifax Data Breach Litigation Suggest Increased Risk of Personal Liability for Directors and Officers for Cybersecurity Incidents

By Freya K. Bowen on February 6, 2019

Despite the increase in data breaches and cyberattacks involving large corporations, efforts to hold directors and officers personally liable for these events have largely been unsuccessful. However, recent developments in two high-profile data breach cases suggest that the relative safety directors and officers have previously experienced from cybersecurity-related suits may be coming to an end. On January 4, 2019, the Superior Court of California approved a $29 million settlement in consolidated derivative litigation brought against directors and officers of Yahoo, Inc. arising out of two data breaches compromising sensitive information of over one billion Yahoo users. *See In re Yahoo! Inc. Shareholder Litig.*, Case No. 17-CV-307054, (Cal. Supp. Ct Jan. 4, 2019). This settlement, which includes a court-approved plaintiff's counsel's fee of $8.6 million, represents the first significant recovery in a data-breach related derivative lawsuit targeting directors and officers for breach of fiduciary duty.

In another closely-watched data breach case against the credit rating firm Equifax, Inc. and certain of its officers and directors, on January 28, 2019, the Northern District of Georgia granted in part and denied in part a motion to dismiss a securities class action arising out of a cyberattack in which criminals gained access to sensitive information of 143 million Equifax customers. ***See In re Equifax, Inc. Secur. Litig.*, Case No. (N.D. Ga. Jan. 28, 2019)**. Although the court granted the motion to dismiss with respect to most of the officers and directors, it denied it as to the Equifax's former CEO, who was alleged to have personal knowledge of the inadequacies in Equifax's cybersecurity system. This ruling makes *Equifax* the first major data-breach related claim against a corporate officer to survive a motion to dismiss.

These cases, along with the increase in cybersecurity-related derivative and securities actions, indicate that directors and officers of major corporations may face an increased risk of personal

liability in connection with data breaches. Companies should bear this risk in mind when analyzing the protections afforded their officers and directors by their insurance programs.

Large corporations have historically protected their officers and directors from personal liability by availing themselves of a Delaware statute that permits corporations to insulate their directors from any alleged violation of the duty of care through a specific exculpatory provision in the certificate of incorporation. ***See* 8 Del. Code § 102(b)(7)**. This provision, however, cannot limit liability for violations of the duty of loyalty, for bad faith acts or omissions, or for knowing violations of the law. *See id.* Moreover, despite general protection from liability for breaches of the duty of care, directors may still face liability for failure to monitor liability-creating activities within the corporation under a "*Caremark* claim," which derives its name from *In re Caremark Int'l Derivative Litigation.,* 698 A.2d 959 (Del. Ch. Ct 1996). Under the *Caremark* standard, a lack of good faith can be established when directors have either (1) utterly failed to implement any reporting or information system or controls; or (2) despite having implemented such a system or controls, consciously failed to monitor or oversee its operations, thus preventing themselves from receiving information about risks requiring their attention. *See Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006). In either case, liability requires a showing that directors failed to act in the face of a known duty to act. *See id.*

The high bar created by the *Caremark* standard has protected directors from personal liability in several prominent data breach cases. For instance, Wyndham, Target, and Home Depot suffered three of the most significant corporate data breaches in recent years. Shareholders of each corporation brought derivative claims against the directors seeking to tie the duty to monitor under *Caremark* to the corporations' cybersecurity systems. The courts granted the defendants' motion to dismiss in each case on the ground that directors' cybersecurity-monitoring duties were not clear enough to form the basis for a *Caremark* claim. *See* ***Palkon v. Holmes*, Case No. 2:14-CV-01234 (D.N.J. Oct. 20, 2014)**; ***Davis et al. v. Target Corp.*, Case No. 14-CV-203 (D. Minn. July 7, 2016) (adopting SLC recommendation to dismiss action)**; ***In re Home Depot, Inc. Shareholder Deriv. Litig.*, 223 F. Supp. 3d 1317 (N.D. Ga. 2016)**.

Now, however, a series of prominent and widely-publicized data breaches, combined with the growth of a cybersecurity industry designed to assist corporations in protecting against cyberattacks, may have created a corporate cybersecurity standard of care that would support a *Caremark* claim. In other words, the very development of stronger cybersecurity protections and controls may have created a known duty to act. The Yahoo data breach derivative litigation could be a harbinger of this trend. Many of the suit's allegations assert a bad-faith failure by the directors to adequately monitor the corporation's cybersecurity system, including through their failure to adequately fund the corporation's data-security infrastructure and through their refusal

to approve necessary security updates. Plaintiffs alleged these lapses left Yahoo's systems vulnerable to attack. The lawsuit also alleged that the directors failed to implement adequate security measures in response to the first data breach. The fact that the suit resulted in a court-approved $29 million settlement, which was fully funded by insurance, indicates that the plaintiffs, defendants, insurance carriers, and the court all agreed that the defendants faced a significant risk of liability.

Likewise, the Equifax data-breach-related securities suit contains numerous allegations of inadequate board oversight of the corporation's cybersecurity systems. The plaintiffs claimed that the company's cybersecurity system was "dangerously deficient" and that the directors and officers failed to implement appropriate security protocols, failed to remediate known deficiencies, and failed to adequately monitor vital systems and networks. The plaintiffs also alleged that the board ignored numerous warnings that its data security measures were inadequate. In its ruling on the motion to dismiss, the court determined that these inadequacies made the company's assurances to investors concerning the security of Equifax's systems materially misleading. The court also determined that the CEO's alleged personal knowledge of the deficiencies in Equifax's cybersecurity systems established the requisite scienter with respect to the alleged misrepresentations concerning the company's data security. The court therefore allowed the claims against the CEO personally to move forward.

Given the increasing risk of personal liability for directors and officers and the considerable damages demanded in high-profile data breach litigation, it is important that a company's directors and officers insurance program adequately protect those individuals from cybersecurity-related liability. This protection is imperative with respect to derivative litigation, as Delaware law precludes a corporation from indemnifying its directors for payment of judgments or settlements in a derivative action. *See* 8 Del. Code § 145(b). Furthermore, any director who has been found liable to the corporation is not entitled to indemnification of defense costs unless a court specifically determines that the director is entitled to such indemnification despite the finding of liability. Thus, a company's Side-A directors and officers insurance program, which provides coverage for non-indemnifiable loss, may be the only protection standing between directors and catastrophic personal liability as a result of a data-breach-related derivative action settlement or judgment.

As a result, risk managers and their coverage counsel should carefully evaluate every directors and officers insurance program for any potential gaps in coverage relating to a cybersecurity event. These gaps may arise from provisions directly referencing cybersecurity, such as an explicit cyber-related exclusion, or from the unanticipated operation of other exclusions and limitations that could be implicated by particular cybersecurity-related claims.

Tech Risk Report

Protecting Innovative Companies Against 21st Century Risks

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Evaluating Your Company's Coverage for Ransomware Attacks Under Its Cyber Insurance Policy

By John Hardin on January 28, 2019

Selecting an appropriate cyber insurance policy can seem daunting. There are a number of different cyber events that have the possibility to impact businesses differently based on a number of factors, including the company's network design and cyber security readiness. The market for cyber insurance policies does not have a widely-accepted form that is predominantly used by carriers, brokers, or policyholders, resulting in approximately 70 carriers drafting their own cyber insurance policies, many of which are negotiable. Lastly, the risks and technology at issue evolve quickly, adding uncertainty and the potential for a "new" event that may not be covered appropriately by your company's current policies.

Indeed, ransomware is a classic example as it soared to "prominence" in recent years only to see cyber criminals rely more on **cryptominers** in the early part of 2018. Nevertheless, by the end of 2018, with cryptocurrency valuation declining, there were signs that the use of miners **had begun to fall**. While, overall, this lead to the decline in "the number of active ransomware families[,] the total number of new variants increased, meaning the ransomware operations that remained active pumped out more samples, more often." And "the chances of ransomware payloads being detected and blocked prior to execution are becoming increasingly low." Ransomware attacks are **expected to reach a global cost of $20 Billion** by 2021.

The following are some (though clearly not all) practical considerations when evaluating your company's coverage for ransomware attacks. First, discuss the deductibles and sublimits related to the cyber extortion coverage with your information technology (IT) department in the context of your network's design and of the impact a successful ransomware attack could have on your network. Many cyber insurance policies contain a deductible that is much higher than the average ransom demanded, while placing a sublimit on cyber extortion coverage that is less than the policy's overall limit and could be less than the overall costs of the attack should the company not be adequately prepared. Policyholders and the appropriate, internal IT liaison should fully discuss

the impact of the deductible and sublimit for ransomware attacks in the context of your company's cyber-incident response strategy, the difficulty in restoring your network from back-up data, and the damages that would result in the interim.

Second, does the policy require notice to the carrier and consent before the ransom is paid? Many policies require advance notice to the carrier and the carrier's consent before paying the ransom. While that may not be an issue for some companies, it can cause issues particularly if the delays in decrypting or restoring the company's data increase the risk of bodily injury or property damage. For example, even minimal delays in decrypting a hospital's data could result in bodily injury or death. Policyholders should consider what actions a policy requires under its extortion coverage before paying a ransom and whether those requirements will impact the company's response and/or its customers if a cyber extortion event occurs.

Third, policyholders should discuss and decide internally if they want to control the outside vendors that are used in the event of a ransomware attack. Many policies require policyholders to select outside vendors such as forensic investigators from a pre-approved list of providers. If your company has selected its vendors and wants to keep them, check the pre-approved list and confirm those vendors are included, or negotiate an appropriate amendment with the carrier.

Fourth, policyholders should carefully evaluate the business interruption coverage under their cyber insurance policies and determine the effectiveness of their policies' responses to the company's particular needs in the aftermath of an attack. For example, is the policy triggered by all cyber events, including cyber-extortion events? Does it adequately cover "extra expenses" to mitigate a loss and the lost business income stemming from an event? Lastly, if your company relies on third-party vendors that are susceptible to similar attacks, does your coverage include contingent or dependent business interruption that will cover your losses if a vendor is impacted by a ransomware attack?

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

The New Money: Cryptocurrencies and the Role of Insurance

By Robert P. Jacobs on January 17, 2019

For approximately the past decade, cryptocurrencies were used by those who wanted to transact business anonymously and without oversight or restrictions imposed by any governmental authority. More recently, the concept of cryptocurrencies has been used to raise capital outside of traditional financial structures. Indeed, the rise of raising money through the issuance of "virtual tokens" using "Initial Coin Offerings" ("ICOs") has caused a sharp rise in the prevalence and market value of cryptocurrencies.

Those involved with cryptocurrencies believe that their virtues include stronger security against theft, easier transactions, and insulation from government-induced currency fluctuations, among other things. But the inescapable reality is that hackers, technical errors, and fraud happen. In addition, regulators have been taking notice and have been attempting to flex their authority, although the manner in which any given regulation applies to cryptocurrencies is far from certain. One thing that is certain, is that the cryptocurrency "industry" poses unique and evolving risk. Given this, the insurance industry is also engaged in attempting address the needs of this emerging market, although underwriters can be expected to rigorously assess the risks posed, and insurance procurement can be a challenge for some.

Regardless, the following is a list of questions that any company engaged in this space should ask itself to determine the lines of insurance it might need and which it should consider.

Does the company need Cyber Insurance?

1. Does the company provide a technology service that might be subject to errors and omissions? For example, a crypto-currency exchange provides a service to its customers that could be subject to mistake that causes a loss.
2. Is there a risk of a privacy breach or breach of privacy regulations?

3. Is there a risk of a security breach with respect to third parties that results in one of the following:
    I. Corruption, destruction or deletion of a third-party's electronic data?
    II. Disclosure of a third party's private information?
    III. Theft of a third party's data?
    IV. Failure to prevent the transmission of malicious code into a third party's network?
4. Is there a risk of a threat of cyber extortion, such as:
    I. A threat to introduce into, or activate malicious code in, a computer system?
    II. A threat that someone will interrupt a computer system?
    III. A threat that someone will damage or destroy a computer system?
    IV. A threat that someone will improperly utilize a computer system or disrupt a network?
5. Is there a risk that some "network" disruption will cause a loss of business income?

Does the company need Commercial Crime Insurance?

1. Is there a risk of employee theft?
2. Is there a risk of vendor theft?
3. Is there a possibility of loss of money or securities through a fraudulent electronic transfer?
4. Is there a risk of "identity fraud" – using a company's or a person's identity to commit a crime?

Does the company need Director's & Officer's Liability Insurance?

1. Is there a risk that a shareholder or investor will allege that an officer or director was guilty of omissions, misstatements, misleading statements, neglect, or breach of duty that resulted in a decrease in the value of stock or other assets such as, possibly, a token?
2. Is there a risk that a shareholder or investor will bring a claim against the company alleging actual or alleged omissions, misstatements, misleading statements, neglect, or breach of duty that violated securities laws and thereby caused a decrease in value of stock or other assets such as, possibly, a token?
3. Is there a risk that a shareholder or investor will demand that the company investigate itself for some corporate wrongdoing for the purposes of determining whether the company should prosecute a derivative action?

4. Is there a risk that a governmental enforcement authority (e.g., SEC, FinCEN) will demand an interview of an officer or director for the purposes of investigating a possible regulatory or other legal violation?

Does the company need Kidnap & Ransom Insurance for some employees?

1. If company employees, particularly directors and officers, travel with “cold storage” wallets (i.e., wallets that are not on-line but, rather, on thumb-drives, etc.), there could be a risk of kidnap or extortion in some regions.

This is, of course, is not meant to present an exhaustive list of all of the types of insurance that any company might need. Those determinations can only be made after a very specific assessment of the role that a company is playing in the crypto-currency space and the risks that it faces. Further, there are nuances to all of these lines of coverage, and the specific coverage provided varies among different insurers. In addition, all companies engaged in the crypto-currency space should expect to undergo fairly rigorous scrutiny by insurance underwriters who will seek to determine, for example, whether a company is at least attempting to be compliant with potentially-applicable regulations and has appropriate safe-guards in place, such as a data security incident response plan.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

False Pretense Exclusion No Bar to Coverage of Fraudulent Impersonation Scams

By Jeff Bowen on January 8, 2019

Social engineering and electronic impersonation scams have increased in recent years, as have cases involving resulting claims for insurance coverage. Claims typically involve the impersonation of a company executive, employee, or client and a fraudulent electronic communication directing an employee of the policyholder to transfer funds to another account. As outlined in our update of November 8, 2017, courts differ significantly as to whether or not this situation triggers coverage under a standard crime policy or fidelity bond. For example, some courts have held that the scheme does not produce a loss "resulting directly" from the "use of a computer" as required for certain "computer fraud" coverage. *E.g.*, *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252, 258 (5th Cir. 2016); *Incomm Holdings, Inc. v. Great Am. Ins. Co.*, No. 1:15-cv-2671-WSD, 2017 WL 1021749, at *8-*10 (N.D. Ga. Mar. 16, 2017). Other courts have reached the opposite conclusion and found coverage. *E.g.*, *Principle Solutions Grp., LLC v. Ironshore Indem., Inc.*, No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *2, *5 (N.D. Ga. Aug. 30, 2016).

Two recent decisions examined an important exclusion in the context of these types of claims and offered additional support for policyholders seeking coverage. In *Rainforest Chocolate, LLC v. Sentinel Insurance Company*, No. 2008-095, 2018 WL 6817065, — A.3d —, 2018 VT 140 (Dec. 28, 2018), the supreme court of Vermont reversed a grant of summary judgment to the insurer, held that the voluntary payments exclusion did not apply, and remanded for consideration of specific coverage grants. In that case, an employee had received an email purportedly from his manager directing an electronic funds transfer to an outside bank account. The policyholder soon discovered the email was fraudulent and submitted an insurance claim for the loss. The district court agreed with the insurer that coverage was barred by the "false pretense" exclusion, which applied to "physical loss or physical damage caused by or resulting from . . . voluntarily parting with any property by you or anyone else to whom you have entrusted the property if induced to do so by any fraudulent scheme, trick, device or false pretense." *Id*. at *1. The supreme court

reversed, holding that the policyholder did not suffer a “physical loss” as required by the exclusion. *Id*. at *5. The court recognized that the policy defined “money” to include funds held in deposit accounts, but found that the policy was subject to different reasonable interpretations as to whether the loss of electronic funds constituted a physical loss. The court therefore construed the ambiguous term against the insurer and remanded the case for consideration of whether the claim fell within one of the policy’s coverage grants.

The *Rainforest* court relied heavily on a similar recent decision from the U.S. District Court in Montana. *Ad Adver. Design, Inc. v. Sentinel Ins. Co.*, No. CV 17-140-BLG-TJC, 2018 WL 4621744, — F.Supp.3d — (D. Mont. Sep. 28, 2018). In that case, the policyholder’s operations manager received four emails purporting to be from the company president that requested electronic payments to an external bank account. The insurer denied coverage for the loss after the fraud was discovered, citing the same “false pretense” exclusion. The district court granted summary judgment to the policyholder after agreeing that the exclusion could be reasonably interpreted not to apply to the loss of electronic funds given the explicit requirement of “physical loss.” *Id*. at *5. While the insurer could reasonably argue that inability to physically access lost funds constituted physical loss, the policy distinguished between “loss” and “physical loss,” permitting the policyholder to reasonably argue that the exclusion was more limited. *Id*. at *4. The court also found coverage under both the “Forgery” and “Money and Securities” coverage provisions, but called for additional briefing on whether the four emails and four resulting transfers constituted one occurrence or four separate occurrences. *Id*. at *6-*7.

The precise language of the exclusion played a critical role in both decisions. The Montana district court suggested that the exclusion would apply in the absence of the “physical loss” language and distinguished three cases applying a different exclusion on that basis. *Id*. at *5 (citing *Schmidt v. Travelers Indem. Co. of Am.*, 101 F. Supp. 3d 768 (S.D. Ohio 2015); *Schweet Linde & Coulson, PLLC v. Travelers Cas. Ins. Co. of Am.*, 2015 WL 3447242 (W.D. Wash. May 28, 2015); *Martin, Shudt, Wallace, Dilorenzo & Johnson v. Travelers Indem. Co. of Conn.*, 2014 WL 460045 (N.D.N.Y. Feb. 5, 2014)). At the same time, the Sixth Circuit recently found coverage for a similar fraudulent email scheme and declined to apply an exclusion for “loss resulting directly or indirectly from the giving or surrendering of Money, Securities or Other Property in any exchange or purchase, whether or not fraudulent, with any other party.” *Am. Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455, 463-64 (6th Cir. 2018). The court held that wire transfers to the impersonator’s account meant there had been no “exchange or purchase” as required by the exclusion. *Id*. Policyholders should therefore carefully examine the language of any “false pretenses” or “voluntary payments” exclusion when negotiating a crime policy or pursuing coverage following a social engineering or phishing scheme.

Apache Corp. v. Great Am. Ins. Co., 662 Fed. Appx. 252, 258 (5th Cir. 2016)

https://caselaw.findlaw.com/us-5th-circuit/1751539.html

Incomm Holdings, Inc. v. Great Am. Ins. Co., No. 1:15-cv-2671-WSD, 2017 WL 1021749, at *8-*10 (N.D. Ga. Mar. 16, 2017).

https://casetext.com/case/incomm-holdings-inc-v-great-am-ins-co-1

Principle Solutions Grp., LLC v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *2, *5 (N.D. Ga. Aug. 30, 2016).

http://propertyinsurancelawobserver.com/wp-content/uploads/sites/11/2016/09/Principle-Solutions-Group-LLC-v.-Ironshore-Indemnity-Inc.pdf

Rainforest Chocolate, LLC v. Sentinel Insurance Company, No. 2008-095, 2018 WL 6817065, — A.3d —, 2018 VT 140 (Dec. 28, 2018)

https://casetext.com/case/rainforest-chocolate-llc-v-sentinel-ins-co

Ad Adver. Design, Inc. v. Sentinel Ins. Co., No. CV 17-140-BLG-TJC, 2018 WL 4621744, — F.Supp.3d — (D. Mont. Sep. 28, 2018).

https://www.executivesummaryblog.com/files/2018/10/Ad-Advertising-Design-v.-Sentinel-Ins.-Co.pdf

Schmidt v. Travelers Indem. Co. of Am., 101 F. Supp. 3d 768 (S.D. Ohio 2015);

https://casetext.com/case/schmidt-v-travelers-indem-co-of-am

Schweet Linde & Coulson, PLLC v. Travelers Cas. Ins. Co. of Am., 2015 WL 3447242 (W.D. Wash. May 28, 2015)

https://www.casemine.com/judgement/us/5914ec53add7b04934949f8f

Martin, Shudt, Wallace, Dilorenzo & Johnson v. Travelers Indem. Co. of Conn., 2014 WL 460045 (N.D.N.Y. Feb. 5, 2014)).

https://casetext.com/case/martin-shudt-wallace

Am. Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 463-64 (6th Cir. 2018).

http://www.opn.ca6.uscourts.gov/opinions.pdf/18a0138p-06.pdf

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Developments in Cyber-Coverage Options

By Norton Cutler on December 20, 2018

The recent series of significant hacks to **Marriott**, **Target**, **Anthem**, **Home Depot**, and other businesses make it clear that there is now another inevitable event to add to death and taxes, namely intrusions to businesses' on-line databases of their customers' personal information. These intrusions include outside vigilante hackers who are simply trying to sell their services and then try to incite the government or private plaintiffs to assert damage claims against the targeted businesses from the exploited vulnerabilities. To counteract the inevitability of such intrusions, cyber-security providers and insurance companies are now considering offering a new product that would combine guarding against unwanted intrusions with guaranteed coverage for the cost of the inevitable hack. The product would basically warrant that there will be no damaging access or release of on-line data, and would provide a specified but limited payment to compensate for any damages should an intrusion and/or release of data nonetheless occur.

Numerous insurance companies already offer some type of high-limit coverage for cyber intrusions, but these policies have significant premiums and contain numerous exclusions for insureds' not taking proper precautions, as well as for various other issues including losses incurred through a breach of contract. Several of these coverage exclusions seem to be headed to the Supreme court for resolution. In the meantime, however, the combined product would provide a service to guard against intrusions that is guaranteed to meet the coverage standards of the insurance company, a correction of any incursion, and a limited payment if the implemented security safeguards are breached and the insured incurs third-party liability. There would be no need to worry about coverage under this type of policy because the security provider is paying the guaranteed amount if there is an incursion and exposure of personal data. The security company would also provide the remediation of any gaps in the insured's system security.

Most security incursions result in little actual out-of-pocket documented damages to the customers whose data is exposed, but the cost of defending lawsuits and implementing

safeguards such as new credit and debit cards, new passports, and identity-theft monitoring provided to the customers whose data was subject to a breach can mount up quickly. The combined product would provide a fixed cost of guarding against a hack and an indemnity payment if one occurs at what will presumably be a lower combined price than having security provided by one firm and insurance by another. There can also be better coordination between the security provider and the insurance provider to improve prevention and lower the cost of remediation. It will be interesting to see how these products, if implemented, roll out and whether they can better prevent intrusions and lower the cost of putting everything back together and compensating the victims. Particularly for businesses that do not already have a security or a cyber-insurance provider, these combined products may well be interesting and have lower cost than separate products. These products would also seem to be especially suited for the healthcare industry where HIPPA provides even more stringent penalties for intrusions and improper protection of patient data.

If a business already has both security and cyber-insurance providers, it could compare the combined cost as well as the experience in coordinating between security provider and insurance and decide whether to consider the combined product. But regardless of what product or products a business ultimately purchases, all businesses that store personal data should take reasonable precautions to protect that data, and should purchase some type of cyber insurance, whether or not it is integrated with a security service.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Will Your Cyber Policy Provide Coverage for GDPR Violations?

By Catherine Del Prete on December 13, 2018

The European Union's Global Data Protection Regulation (GDPR) took effect on May 25, 2018, and drastically expanded the compliance obligations of companies involved in the collection, use, and management of any European Union citizens' data. The GDPR imposes a strict regulatory scheme with steep penalties for non-compliance, with maximum fines set at the greater of 20 million Euros or 4% of a company's annual worldwide revenue. **GDPR Art. 83, § 5**. Please refer to Perkins Coie's **GDPR Resources** for a more comprehensive overview.

Companies should look critically at their insurance coverage to ensure their cyber policies provide adequate coverage in the event of an action under the GDPR. Below we identify general concepts that should be assessed when reviewing cyber policies for GDPR coverage. Because every insurance policy is unique (especially with respect to cyber coverage), this list is not meant to be exhaustive, but instead to provide a conceptual framework for a review of your company's coverage.

- **Definition of Personal Information**: The GDPR regulates "personal data" which is defined broadly to include "any information [directly or indirectly] relating to an identified or identifiable natural person[.]" **GDPR Art. 4, § 1**. The definition of "personal information" (sometimes referred to as "personally identifiable information" or "private information") in your cyber policy should be as broad as possible to ensure that there are no gaps between potential actions under the GDPR and what is covered by your policy.
- **Coverage for privacy law violations**: Cyber policies typically provide coverage for costs arising from a cyber breach. With the passage of the GDPR, however, mere wrongful collection or storage of an individual's information is a violation of the law and can be the basis for a regulatory investigation and proceeding. Confirm that your company's cyber policy provides coverage for violations of privacy laws, regardless of whether a breach is involved. Check to ensure your policy does not contain any exclusions for claims arising

from activities regulated by the GDPR. Further, ensure that regulatory actions covered by your policy can be instituted by “any” governmental entity or by “any international” governmental entity — coverage that is restricted to actions brought by U.S. governmental or state entities will not provide coverage for GDPR violations.

- **Coverage for fines and penalties**: Many cyber policies provide coverage for fines and penalties arising from privacy breaches, including violations relating to a company’s non-compliance with privacy breach notification laws. Because the GDPR imposes fines on companies for non-privacy breach activities, including the improper collection and storage of data, it is important that your cyber policy’s scope of regulatory damages be expansive. Check your policy to ensure that regulatory coverage is broad and applies to any violation of a privacy law or regulation.
- **Most favored nations clause**: The insurability of fines and penalties varies based on jurisdiction. Your cyber policy should have language to ensure any fines and penalties are covered to the fullest extent permissible under the law of the most favorable jurisdiction, otherwise known as a “most favored nations” clause.
- **Cyber Limits**: The GDPR permits onerous fines for violations. Be sure to take a close look at your cyber coverage limits in light of potential for increased fines under the GDPR. Many cyber policies have sublimits for regulatory fines and penalties — ensure that any sublimited coverage is adequate with respect to your company’s needs.

Finally, be critical of any endorsements purporting to add GDPR coverage to your cyber policy. Some carriers have attempted to address issues with GDPR coverage by including an endorsement to cyber policies that simply includes coverage for claims arising out of the GDPR regulations, subject to the terms and conditions of the policy. These endorsements do not address the issues set forth above and often leave policyholders without coverage for the vast majority of GDPR violations.

Conducting a careful analysis of your cyber coverage will prove invaluable in the event of a GDPR violation. As cyber claims arising from the GDPR begin to roll in, new issues will invariably arise from a coverage perspective. Continuing to monitor developments in GDPR trends and coverage issues is vital to ensure that your company is adequately protected.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

How Valuable is that Certificate of Insurance?

By Jay Rossiter on December 10, 2018

On November 9, 2018, the Ninth Circuit certified an important coverage question to the Washington Supreme Court about whether a certificate of insurance (COI) purporting to add T-Mobile as an additional insured on another company's insurance policy binds the insurance company listed on the certificate. *T-Mobile USA Inc. v. Selective Insurance Company of America*, 908 F.3d 581 (9th Cir. 2018).

The case should serve as a reminder that businesses may not be able to rely on, and should not rely on, a certificate of insurance alone when they sign agreements with third parties who are supposed to add them as additional insureds.

In the *T-Mobile* case, a regional subsidiary of T-Mobile entered into an agreement with a company called Innovative Engineering, relating to the construction of rooftop cellular antennae towers in New York City. The agreement required Innovative, among other things, to maintain general liability insurance naming the T-Mobile subsidiary as an additional insured. T-Mobile was provided with a certificate of insurance that appeared to show that T-Mobile was covered as an additional insured under Innovative's insurance policy. When a property damage claim later arose, T-Mobile tendered the claim to Innovative, requesting that Innovative notify its insurance company, Selective Insurance Company of America. Selective denied T-Mobile's claim on the grounds that T-Mobile was not named as an insured and did not qualified as an additional insured.

The Ninth Circuit acknowledged that a certificate of insurance alone under Washington law does not change the terms of an insurance policy, where the insurance policy does not also provide coverage for an additional insured: "[A] COI is *not* the functional equivalent of an insurance policy, and it therefore *cannot* be used to amend, extend, or alter the coverage provisions of an insurance policy." 908 F.3d at 585 (emphasis in the original). *See also Postlewait Constr. Inc. v. Great Am. Ins. Cos.*, 106 Wn.2d 96, 100-01 (1986); *Int'l Marine Underwriters v. ABCD Marine, LLC,* 165 Wn. App. 223, 233 (2011). Here, however, it was the insurance company's own agent

that had assured T-Mobile that it would be covered as an additional insured. As such, the Ninth Circuit recognized that Washington law also provided that "an insurance company is bound by all acts, contracts, or representations of its agent, whether general or special, which are within the scope of [the agent's] real or apparent authority." 908 F.3d at 585, quoting *Chicago Title Ins. Co. v. Wash. State Office of Ins. Comm'r*, 178 Wn.2d 120, 136 (2013). In light of these competing Washington authorities, the Ninth Circuit certified the question to the Washington Supreme Court.

The *T-Mobile* case is unique because it turns on representations made by the insurance company's own agent. But, for the vast majority of certificates out there, and uniformly across U.S. jurisdictions, the COI itself does not actually provide any insurance.

How do you protect yourself? Insist on seeing the insurance policy endorsement that actually extends coverage to your business and adds you as an additional insured. If the third party promised to add you, and obtained a certificate for you, you might think you are covered. But unless you actually confirm the coverage, you may be out of luck. You might have a claim for breach of contract against the third party, but that might only go so far if the third party has limited assets. It is much better to have the financial resources of an insurance company to protect you. By reviewing the underlying policy or endorsement, you will also be able to make an informed decision about whether you need to beef up your own insurance to address future risks.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Protecting Your Emerging Business

By Jay Rossiter on December 7, 2018

Emerging tech companies face many uncertainties. On the one hand, it's an exciting environment with eager investors and an expanding market receptive to new high-tech solutions. But there are also risks from cyber disruption, potential product liability claims, and less than trustworthy vendors. Don't get caught without adequate protections.

Indemnification agreements. Carefully drafted indemnity provisions in your contracts with vendors and other third parties, including suppliers and large customers, can go a long way to protecting your business against various risks that are out of your control. When a claim arises, you will want the indemnitor to step in to address issues as seamlessly as possible. Close attention to the details of your agreements is critical. Don't rely on standard form provisions that are not tailored to your business. If a dispute arises, you will want to make sure, for example, that you are not bogged down by unfavorable choice-of-law or dispute-resolution provisions. These should be addressed in advance. Keep in mind that an indemnity agreement is only as good as the indemnitor who signs it. If the indemnitor is insolvent or unwilling to step up, then your business is on its own. Insurance is the only way to provide that additional security.

Insurance provisions. Indemnity provisions in your agreements can and should be supplemented by an insurance provision that requires the other party to maintain minimal levels of insurance and to name your business as an additional insured. This can provide an additional layer of protection. But, insurance provisions can represent a false sense of security, so beware. Unless you actually request a copy of the other party's insurance policy and review it in advance, there is no way to know how strong the coverage will be. Many insurance companies severely limit their obligations when it comes to additional insureds under their policies and may include exclusions or other limitations that make coverage as an additional insured for future claims unlikely. Relying upon a certificate of insurance alone without seeing the underlying policy can also be risky, even if the certificate says that your company is an additional insured. Generally,

the insurance policy alone controls. If you can, ask for the policy or endorsement that is referenced in the certificate. That is the only way to make sure you are protected.

Products/completed operations insurance. Many companies rely on their brokers to obtain a basic insurance package to address business risks. Depending on what stage your business is in, you might not be able to afford anything but the most basic insurance, with modest limits at affordable premiums. But be aware that many standard liability policies specifically exclude coverage for product claims. If you are selling a product or a component part incorporated into another's product, you are at risk for product claims. Your liability insurance may actually provide no protection at all. Review it carefully so that you can make an informed decision about that risk and enhance your coverage as necessary at the time of renewal.

Specialized insurance. Your basic business insurance generally includes property insurance, general liability coverage, auto liability coverage, and certain employment-related insurance, like workers comp. Directors and officers (D&O) insurance is also a must-have, and for private companies, the coverage extends to your business as well as your Ds and Os. As your company grows, and as it specializes in certain areas, other lines of insurance can provide additional security. These include cyber coverage, media coverage, technology errors and omissions coverage, and more robust forms of employment practices insurance.

Your business model is unique. That is what caught the eye of investors and gives you an edge in the marketplace. You may also need to be creative and think outside the box in addressing potential risks. That off-the-shelf, cookie-cutter insurance package suggested by your broker may not actually capture your company's unique risks.

Welcome to The Perkins Coie Tech Risk Report

By Karin Scherner Aldama, Robert P. Jacobs & Jay Rossiter on December 6, 2018

Welcome to The Perkins Coie Tech Risk Report, a source for updates on, and analysis and interpretation of, insurance issues relevant to emerging technologies. We will address coverage issues related to cyber coverage, privacy, digital assets like cryptocurrency, Blockchain and other emerging technologies. The blog is written for start-ups and other companies dealing with emerging issues in the technology industry.

Attorneys from Perkins Coie's Insurance Recovery Group will be the primary content authors. They will be joined from time to time by attorneys from other practice groups, such as the firm's Blockchain and Virtual Currency, Emerging Companies, Technology Transactions and Privacy and Data Security practice groups.

Please **sign up to receive our postings**. We welcome your feedback, comments, and questions, and we look forward to our conversations. Thank you for visiting!

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Coverage for Third-Party Claims Alleging Non-Fax-Related TCPA Violations

By Perkins Coie on November 10, 2017

The Los Angeles Lakers are still dealing with the fallout from having sent confirmatory text messages to spectators in 2013, after having invited text messages from those spectators for potential display on the scoreboard. The ensuing Telephone Consumer Protection Act (TCPA) class action settled, but the Lakers' suit against its insurer seeking coverage for defense costs and indemnification remains pending. The outcome of this dispute could have deep implications for any business using text messaging as part of its platform.

Oral argument in the Lakers' appeal from the district court's judgment of no coverage was held on February 15, 2017, with the opinion pending. *See* **Recording of oral argument in *LA Lakers v. Fed. Ins. Co.*, No. 15-55777 (9th Cir.).**At issue in the case is whether Federal Insurance Company (Federal) had to defend and indemnify the Lakers with respect to the underlying class action (the Class Action) under the Lakers' Directors and Officers policy (the Policy). The district court ruled that there was no coverage because TCPA claims are by definition claims for invasion of privacy, and such claims fall under the Policy's exclusion for claims against the Lakers "based on, arising from, or in consequence of . . . invasion of privacy." *Los Angeles Lakers, Inc. v. Fed. Ins. Co.*, No. CV 15-7743 DMG (SHx), 2015 WL 2088865 (C.D. Cal. Apr. 17, 2015). On appeal, the parties' central positions are laid out below.

Arguments on Appeal of *LA Lakers v. Fed. Ins. Co*

The Lakers' main argument is that the TCPA's language, its legislative history, and FCC comments to its implementing regulations make clear that protection against invasions of privacy is not the TCPA's only purpose, but that it was also intended to protect consumers from the nuisance and costs associated with prohibited phone calls (both actual charges for incoming messages and diminution in paid-for plan minutes or message limits).

Since, according to the Lakers, the Class Action plaintiff based his TCPA claim on the costs and lost minutes resulting from the Lakers' text, the district court's conclusion that the invasion of privacy exclusion applied was incorrect. And even if some aspect of the Class Action claim was related to invasion of privacy, there was also the economic/nuisance claim, obliging Federal to defend (though not indemnify) the entire Class Action. The Lakers also argue that the exclusion is ambiguous (and has to be construed in favor of the Lakers) because it merely contains a list of torts, so that a reasonable insured would not understand it to apply to statutory TCPA claims, especially since other exclusions specifically mention statutory claims.

Federal, on the other hand, argues that TCPA claims are inherently claims relating to invasions of privacy, and that the references to "nuisances" in the legislative history and elsewhere are best understood in their natural reading as something "annoying," and not a term of art referencing a tort.

Moreover, the underlying complaint mentioned "invasion of privacy" repeatedly, so that its claims are at the very least "based upon, or arising from or in consequence of" such an invasion and hence fall under the broad language of the exclusion. Federal also contends that the exclusion is not ambiguous because the term "invasion of privacy" has a readily understood meaning that applies to things such as unwanted, intrusive phone calls and text messages.

Finally, Federal seeks to distinguish the precedent on which the Lakers rely to argue that courts have found coverage for TCPA claims as property damage or a private nuisance because those cases implicated commercial general liability (CGL) policies with different wording—according to Federal, all cases addressing coverage for TCPA claims under D&O policies have found no coverage.

At the February 15, 2017 oral argument, the judges focused on whether a TCPA claim is one for invasion of privacy only or could comprise other types of claims, like ones for nuisance, and on whether the Class Action complaint sufficiently pled a nuisance claim. From the argument (and trying to read the tea leaves), it sounds as if the panel was inclined to uphold the district court's decision because (1) a TCPA claim is one for invasion of privacy; (2) even if a TCPA claim could be a claim for nuisance, the Class Action complaint did not properly plead that; and (3) even if there were a nuisance claim, it would be in consequence of the invasion of privacy and thus still fall under the exclusion.

Such an outcome would reinforce the dichotomy for which Federal argued on appeal, namely that there is no coverage for TCPA claims under D&O policies because those generally include invasion-of-privacy-related exclusions, while there *may* be coverage for TCPA claims under CGL

policies, which typically provide coverage for accidental property damage and for advertising injury defined as including invasion of privacy. The “may” in the preceding sentence is important though: Caselaw on the issue of TCPA-claim coverage under CGL policies is all over the map, generally depending on the relevant policy language.

Caselaw Lessons

A few principles that emerge from the cases, the vast majority of which concern junk faxes as opposed to unauthorized calls or text messages, are as follows:

To the extent that CGL policies define property-damage-related occurrences as having to be “accidental,” the majority of courts finds that there is no coverage for TCPA claims because the advertiser intends, or at least knows, that the injury will result from its conduct. *E.g.*, ***Am. States Ins. Co. v. Capital Assocs. of Jackson County, Inc.***, 392 F.3d 939 (7th Cir. 2004). One notable exception to this principle is ***Park University Enterprises v. American Casualty Co. of Reading***, 314 F. Supp. 2d 1094, 1101-05 (D. Kan. 2004), where the court found that there was a duty to defend on the basis of property damage because the underlying complaint alleged negligence, which the court considered an accidental event.

As to advertising injury, courts often find that there is no coverage because CGL policies address only the right to secrecy (i.e., not to have private information published), whereas the TCPA is concerned only with the right to seclusion (i.e., to be free from unwarranted intrusion)—at least where the policy defines advertising injury as requiring something along the lines of the “making known . . . of material that violates an individual’s right to privacy.” *E.g.*, ***ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co.***, 147 Cal. App. 4th 137, 147-49 (2007). But where that definition only requires the “oral or written publication” of such material (without the “making known” language), courts have split, with some finding potential coverage and others not. *Compare* ***State Farm Gen. Ins. Co. v. JT’s Frames, Inc.***, 181 Cal. App. 4th 429, 447 (2010), *with* ***Owners Ins. Co. v. European Auto Works, Inc.*****,** 695 F.3d 814, 817-20 (8th Cir. 2012).

Overall, the best that can be said for now is that it is likely easier to obtain coverage for TCPA claims under CGL policies than under D&O policies (though there are now some CGL policies that specifically exclude coverage for TCPA claims), and that that may, but currently does not appear too likely to, change depending on how the U.S. Court of Appeals for the Ninth Circuit rules on the Lakers’ appeal.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

How to Protect Against Cyber Liability Threats

By Perkins Coie on November 8, 2017

The potential for cyberattacks and data breaches continues to loom large in any company's calculus of risk, with events like the recent WannaCry attack only highlighting the threat. For years, the insurance industry has responded in kind by offering variations on forms of cyber risk insurance. However, not all policies are created equal. It is important for the insured to be aware of what is covered—and what is not.

At its most basic level, cyber risk insurance can be divided into first-party and third-party coverages. Most policies will contain some combination of these coverage types. Both of these coverages potentially contain pitfalls for the unwary.

First-party coverage. This concerns loss suffered by the insured, such as losses due to cyber theft and cyber extortion/ransomware. Insureds should look for policies that also cover losses due to network business interruption and include data loss protection as well as forensic investigation coverage (i.e., determining the cause of the loss). Paying for the cost of an intensive internal investigation of system vulnerabilities may be the most valuable benefit of first-party coverage.

Recent ransomware incidents highlight how crippling malicious code can be to your business. And if your business depends on its online links to customers, you will want to ensure broad coverage for "threats and extortion" within your cyber policy, including payment of ransom costs in an extortion scenario.

Common exclusions that the insured would do well to avoid are (1) exclusions for self-propagating code; (2) war and/or terrorism exclusions, which could prevent coverage if the attack came from some unknown foreign source; and (3) certain exclusions for failure to maintain minimum safety standards, which may be vaguely defined and difficult to maintain in practice.

Third-party coverage. This coverage concerns losses suffered by third parties for which the insured is liable, such as losses suffered for a breach in the insured's network security (i.e.,

network security liability) and losses due to the insured's failure to protect a third-party's confidential information (i.e., privacy liability). An insured should consider whether its policy covers regulatory actions, and if so, whether coverage is only triggered by a "suit," which would mean that the insured would not have coverage for the frequently expensive investigative stage of a governmental action. Some policies also cover costs associated with the after-effects of any network security or privacy breach, such as the cost of notifying third parties affected by the breach, costs of ongoing credit or identity monitoring of affected third parties, and costs of hiring a PR firm to protect the insured company's image.

If a Cyber Threat Appears

If you become aware of any cyber threat whatsoever, it is imperative that you contact your insurance providers as soon as possible. If you have purchased stand-alone cyber insurance, for example, the insurer may have forensic experts lined up to assist in addressing any breach situation. Even if you do not have a stand-alone cyber policy, you should check your commercial liability insurance (including general liability, D&O or professional liability), media policies and/or kidnap and ransom coverage. Depending upon the facts, these other policies might be implicated by a cyber risk or claim.

Although the above provides a broad overview of cyber risk insurance, as with any type of insurance, the devil is in the details. Any purchase of insurance carries with it some degree of uncertainty, but this can be limited by having your potential policy closely reviewed by a specialist in the field. And should the day ultimately arise when a cyber loss occurs, having your policy assessed by an experienced insurance litigator could help make sure your company gets the best coverage result possible.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

What's the Insurance Coverage for Smart Contracts?

By Perkins Coie on November 8, 2017

Smart contracts are changing the way businesses conduct routine transactions to make them more efficient and, in many ways, less prone to human error. But this new technology has associated risks. Is your company adequately prepared?

Basics of Smart Contracts

Smart contracts, sometimes known as self-executing contracts, are contracts that are written in computer code and connected to a blockchain so that an individual or entity can instantly be bound to the terms of the contract. Computing devices may also be bound via a smart contract, which has led to the Internet of Things.

The groundbreaking nature of smart contracts is that contracts that previously depended on human interaction, and the accompanying room for error and delay, are now self-executing. For example, a smart contract could be used to handle escrow payments or to evaluate loan eligibility — simply input your information and then your application is automatically approved or denied. An individual does not need to release the funds or to approve the loan. The range of the utility of smart contracts is still being explored. As smart contracts are associated with blockchains, essentially anything that relies or could rely on a ledger could potentially be handled via smart contract.

Possible Risks

Given that the intent of smart contracts is to reduce risk and enhance speed, what are the risks to consider when thinking about coverage?

First, as with anything associated with blockchain technology or computing in general, an error in code could cause loss to the person or entity affected. The error could take place either in the

code to set up the blockchain on which the smart contract depends or the code that programmed the smart contract itself.

In addition, contracts with escape clauses may be more susceptible to error, as the power to invoke these clauses resides with individuals who could use them in such a way as to throw off the transaction and nullify the smart contract. Errors of this sort have already been known to happen. For example, a Canadian digital currency exchange called QuadrigaCX reported that a malfunction in a smart contract code prevented the smart contract from operating and caused a loss of $14 million in the cryptocurrency ether.

Errors in smart contracts have been known to happen to devastating effect. In 2016, a hack in an Ethereum (a type of cryptocurrency) smart contract caused the smart contract to act recursively, so that the act of sending funds triggered a corresponding request to send funds. Losses from this hack are estimated to total $150 million. Part of the reason for the high costs is because smart contracts are immutable and can only be replaced by another smart contract. This is generally seen as one of the benefits of smart contracts, i.e. that they cannot be tampered with. Although this often is favorable, it also means that, when an error takes place, it is permanent.

Businesses can—and should—pursue best practices to mitigate these risks, such as using smart contracts that have been tested by other companies and running any potential smart contracts through as an exhaustive series of tests as possible. Regardless, risk can still remain.

Current and Future Coverages

Coverage for errors with smart contracts can be tricky and will depend on the facts and circumstances of a given loss.

Typically, loss from a smart contract does not occur to a third party, meaning that liability coverage does not apply under most scenarios. First-party coverages could apply, however, if the circumstances so warrant. Loss that occurs as the result of hacking could be covered as cyber theft and/or cyber extortion, either under a stand-alone cyber policy or as an add-on to other types of coverage. If the error resulted in a loss of company property, more traditional coverages could be pursued. If the error is due to a coding deficiency in code written by an employee, however, the risk could be excluded under an employee exclusion.

Perhaps the most important takeaway, however, is not what coverage there currently is but what coverage companies should seek in the future. Smart contracts are here to stay, and insurance for risks associated with smart contracts may be a hot topic in coming years.

Tech Risk Report

Protecting Innovative Companies Against 21st Century Risks

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Social Engineering Fraud: Can You Expect Coverage?

By Perkins Coie on November 8, 2017

In an all too common scenario, someone in your organization's finance department receives an email that purports to be from a supplier informing your organization of the supplier's supposedly changed bank account and a request for you to make all future payments to the new account. Even after some likely back and forth via phone and/or email with the "supplier," your employee ultimately changes the payment information in your systems, and future invoices are paid to the new pay-to account. Everything seems fine for a while, and then the problems begin.

Eventually, your company receives an email from the supplier asking why it hasn't received payment of its recent invoices. When the supplier insists that it has not received payment, in spite of your company's assurances that all invoices have been paid, your IT department investigates. The IT team figures out that the emails with the new payment information and the phone calls were fraudulent—they were not from your supplier but from a bad actor. It is, of course, too late to recover the fraudulently obtained payments, and in the interest of keeping the supplier, your company pays again.

What happens next? Tracking down the bad actor is generally difficult, if not impossible—he or she knows how to cover his or her tracks. But you realize that your company has a crime insurance policy that provides coverage for events like computer fraud. Surely, your insurer must have to cover the double payment and related costs under those provisions, right?

Unfortunately, the answer is "maybe," at best.

With the increasing prevalence of what is called "social engineering fraud," the scope of coverage for such frauds under crime policies is, and has been, the subject of a lot of litigation. Unfortunately, many of the decisions that have thus far been rendered are not encouraging for policyholders.

Computer Fraud Coverage

Computer fraud provisions in crime policies often provide coverage for “loss of . . . money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property . . . .”

Many courts have held that there is no coverage for social engineering fraud under such provisions because the losses resulting from such frauds do not “result directly” from the use of a computer.

For example, in *Apache Corp. v. Great American Insurance Co.*, the insured had, after receipt of a fraudulent email containing updated payment instructions, looked to some extent into the alleged vendor’s request to change its banking information, authorized the change and the payments pursuant to valid invoices, and initiated the payments. The court did not consider those payments to be a direct enough result of the computer use to generate the fraudulent email for computer fraud coverage to be available. 662 F. App’x 252, 258-59 (5th Cir. 2016) (per curiam, unpublished opinion). Rather, the court concluded that “the transfers were made not because of fraudulent information, but because [the insured] elected to pay legitimate invoices,” albeit to a fraudulent bank account; that is, “the invoices, not the [fraudulent] email, were the reason for the fund transfers.” *Id.* at 259; *see also, e.g.*, *Incomm Holdings, Inc. v. Great Am. Ins. Co.*, No. 1:15-cv-2671-WSD, 2017 WL 1021749, at *8-*10 (N.D. Ga. Mar. 16, 2017) (Losses did not result directly from use of computer because they occurred only when charges were subsequently made, that is, as a result of further human activity.)

Similarly, even where a court assumed that the “direct result” requirement was satisfied, it found no coverage because of an exclusion for “loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured’s Computer System.” *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, No. C14-1368RSL, 2016 WL 3655265, at *2 (W.D. Wash. July 8, 2016).[1] Because an employee of the insured had entered the fraudulent banking information into the insured’s computer system, the exclusion applied. *Id.* at *1, *3; *see also Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App’x 627 (9th Cir. 2017) (no coverage for social engineering fraud where policy required unauthorized entry into insured’s computer system because spoofed email did not constitute such entry).

Hope for Policyholders

There are, however, a few cases that should provide some hope to policyholders. Thus, one court has explicitly rejected the reasoning of *Apache,* finding insufficient direct causation, stating that “the Court finds [*Apache*’s] causation analysis unpersuasive,” and holding that the insured’s “employees only initiated the transfer as a direct cause of the thief sending spoof[ed] emails” with

fraudulent transfer instructions. *Medidata Solutions., Inc. v. Fed. Ins. Co.*, No. 1:15-cv-00907-ALC (S.D.N.Y. July 21, 2017) (granting summary judgment to insured under crime policy for $4.7 million loss resulting from social engineering fraud).[2]

Similarly, in *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, the court held that the insured was entitled to coverage under a crime policy containing a "direct result" requirement even though a company employee had acted upon the fraudulent instructions and initiated the wire transfer at issue because "[i]t is reasonable for [the insured] to interpret the language of the policy to provide coverage even if there were intervening events between the fraud and the loss." No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *2, *5 (N.D. Ga. Aug. 30, 2016). Although the court found the insurer's interpretation requiring a more direct linkage between the fraud and the loss also reasonable, it concluded that, "[i]n this circumstance, the Court must construe the policy in the light most favorable to [insured] and provide coverage." *Id.*

What's the takeaway? If your crime policy contains any type of "direct result" requirement in its computer fraud provision, you may not be able to obtain coverage for social engineering fraud under that provision because social engineering fraud typically involves some action by the insured or third parties between receipt of the fraudulent or spoofed information and the transfer of funds resulting in a loss. If that is a concern, the solution may be an endorsement to your crime policy or a cyber policy (with an endorsement, if necessary) that explicitly provides coverage for social engineering fraud.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

How to Maximize Protection Under Additional Insured Provisions

By Perkins Coie on November 7, 2017

Many contracts require that parties be added as “additional insureds,” but few contain specifics on what type of coverage should be provided. The gambit of additional insured provisions is far-ranging. Being proactive and ensuring that the additional insured coverage you are expecting is *actually* provided on the front end will eliminate a host of issues should you need to invoke coverage under the provision.

Additional insured coverage is normally provided by endorsement, at times listing specific entities or individuals and at other times providing blanket coverage for all that require it via contract. In theory, being included as an additional insured provides protection as if your company was a named insured on another’s policy. In reality, however, there are many variations of additional insured coverage that often contain restrictions on the rights of additional insureds under the policies.

Although your contracts may require that you receive certificates of insurance evidencing insurance coverage from the co-contracting party, certificates of insurance rarely, if ever, provide details on the specifics of additional insured coverage. In any contract where your company seeks to be added as an additional insured under another’s policy, it is a best practice that you receive a copy of the additional insured coverage provision before entering into the contract. If, however, the other party is unwilling to provide the policy language, you should include specifics in the contract to help ensure you are adequately covered.

Limitations of Activities or Products. Some additional insured endorsements limit coverage to certain loss amounts or to certain activities and products. If you are concerned about coverage for an activity your company performs or a product your company makes, be sure to include a provision that the specified activity will be included under the scope of additional insured coverage.

Primary Coverage. Some additional insured provisions provide that the additional insured coverage is “primary” and non-contributory, which means that the other party’s insurer will pay first on the claim. However, many additional insured provisions state that the coverage provided is excess to any other insurance available to an insured. Including a condition in your contract that the additional insured coverage states that it is “primary” and non-contributory coverage is helpful to preemptively avoid disputes between your primary carrier and your vendor’s carrier vis-á-vis other insurance clauses.

Ongoing and Completed Operations. Depending on the type of work your company performs, there could be potential liability to your company after the performance on the contract is completed. If so, then any additional insured coverage should specify that it is for both ongoing and completed operations, as many coverages can be limited to ongoing operations.

Coverage Provided. Several additional insured endorsements provide coverage under only certain coverage parts of the policy. For example, in many Commercial General Liability policies, additional insured provisions may only apply to claims arising from bodily injury or property damage, but not for personal and advertising injuries.

Insured vs. Insured Coverage. Many insurance policies contain exclusions for “insured vs. insured” claims, meaning that claims by one insured against another are barred by the policy. Reviewing additional insured coverage and this exclusion is essential to ensure that coverage is not barred for claims by your company against the other party providing coverage.

Additional insured coverage is common in contracts and is frequently provided by insurers, but there is a wide variation of what type of coverage is actually provided. Requiring that your additional insured coverage contains specific coverage options is an essential starting point to ensure your company is adequately covered. In addition, reviewing the coverage actually provided will permit you to catch any unique coverage aspects that could limit your additional insured status under the policy. Being proactive when your company is added as an additional insured will ensure that you obtain the coverage bargained for as part of your contract, in addition to avoiding costly coverage disputes in the event of a claim.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Attack of the Drones: How to Protect Your Business

By Perkins Coie on November 7, 2017

Thinking about including an unmanned aerial vehicle as part of your business? What could be cooler than having a UAV deliver your product to customers? Many companies are already using UAVs or drones not only for delivery but also for video surveillance, property surveying for agriculture or unique promotional videos. Your business will want to consider the basic rules for drone operation—like having an experienced pilot and a well-maintained drone— as well as other ways to manage potential risks.

Possible Risks

There are a number of risks if your business has a connection to drones. What happens if a drone crashes or if a bystander shoots it down? In the evolving high-tech world, there are also real threats of someone hacking into your remote system and interfering with your controls. If there is a crash, there is a possibility you might be liable for the property of others. Drones can be a significant investment, and you will want to protect your asset and yourself if someone blames you for some loss.

There is also a risk that a drone could accidentally harm someone. The technology is advancing, but people have been hurt by propeller blades or by drones flying too close to heavily populated areas. For example, at a concert in Mexico in 2015 in front of thousands of fans, pop star Enrique Iglesias reached out to grab a drone that had been used to take video of his performance, only to accidentally grab a propeller by mistake, partially severing his finger.

With advances in video and audio technology, drones can be used to capture minute details that could inadvertently infringe on another’s privacy rights. For example, a surveillance camera affixed to a drone could capture images in a fly-by that are downloaded and posted to YouTube without the permission of a private party.

Couple this with other risks, like damage to cargo (if the drone is used to transport packages) or accidentally trespassing on someone's property, and it's apparent how these cool new devices create potentially thorny legal issues. You might face liability if your business operates the drones, or if you hire an operator to perform the services for you.

Protect Your Business

There are a number of ways to protect your business. This includes paying attention to safe operation and maintenance. If you hire others to provide UAV services, you should be careful to include specific indemnification language in your agreement and require that vendors maintain proper insurance. Having the right insurance will also protect your business against unforeseen risks.

Having general liability insurance will not guarantee that you are protected. Standard policy forms exclude injuries and damages "resulting from the ownership, maintenance, or use of aircraft." Even though the FAA issued regulations in 2016 relating to drones, which may be of assistance in the ultimate interpretation of insurance provisions that exclude aircraft, there are still uncertainties as to how and whether standard forms apply to drone liabilities. Nevertheless, in 2015, the insurance industry introduced new endorsements that specifically address "unmanned aircraft." Many of the endorsements can be added by insurers to specifically exclude drone liability. There are other endorsements that extend coverage for UAV operations that are specifically scheduled in the endorsement. If your business will include or involve drones as part of its future operations, you will want to examine any proposed forms closely before the insurance is finalized to make sure that you are protected. These forms might or might not protect you against privacy, trespass or nuisance claims. If you are undecided as to whether you need cyber coverage for your business, keep in mind that the information gathered by a drone can be hacked or misused, and cyber liability policies might be the best way to protect against these risks.

Specialty Drone Insurance

With the emergence of more widespread drone use, there has been the development of specialty drone insurance products, particularly by insurance companies with significant preexisting experience in the aviation insurance market.

If your business model involves significant UAV operations, you are well advised to explore the specialty products offered by companies like Global Aerospace, Berkley Aviation, Lloyds and AIG with your broker. Consistent with the high-paced technical world, there is also more limited specialty drone coverage that can be purchased on a flight-by-flight basis. You can download an app from Verifly, for example, that provides up to eight hours of insurance coverage for specific

drone operations based on various criteria that you provide in your response to prompts within the app.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Prepare for the Future With Cryptocurrency Insurance

By Perkins Coie on November 7, 2017

Cryptocurrencies, including bitcoin, may be the wave of the future, as more and more companies and countries accept them as valid forms of currency. As with any new technology, however, the potential for risk and error is prevalent. Although cryptocurrencies are backed by various blockchains designed to reduce risk, a certain amount of risk is unavoidable. And where there is risk, insurance follows.

For example, the Mt. Gox scandal, which is speculated to involve a bitcoin insider taking bitcoins from the exchange, is estimated to result in losses of more than $400 million. Traditionally, insureds attempted to find coverage for risks related to cryptocurrencies by finding novel constructions of provisions in extant insurance policies. Often, the insured was simply left without any coverage. But certain insurers have begun taking the bull by the horns and marketing a new kind of product—cryptocurrency insurance.

Available Cryptocurrency Coverage

In 2014, Great American Insurance Company began to offer the first official Bitcoin Insurance coverage to businesses. Specifically, Great American began granting endorsements to existing crime policies for customers who accept bitcoin for additional crime insurance. The Great American policy covers Employee Dishonesty, Money & Securities Forgery and Computer Fraud, with additional coverages available as endorsements.

Additional cryptocurrency coverage options arrived in 2015, including when Bitcoin Financial Group, LLC began to offer various insurance products for insureds through a special service called BitSecure. The coverage offered by BitSecure is tailored to the needs of the particular insured but, broadly speaking, is designed to be broader than the crime coverage offered by Great American.

Insurance is also being offered by companies like Coinbase, Inc. and Elliptic Enterprise Ltd. for bitcoin storage. These policies are currently somewhat limited, however, and the specifics of coverage vary depending on the company that is offering it. In general, these policies will protect a company from theft as well as losses resulting from errors in the technology used to provide whatever service the company offers.

The availability of cryptocurrency insurance is growing. In November 2016, Mitsui Sumitomo Insurance began offering cryptocurrency insurance to cryptocurrency exchanges. The Mitsui policy covers loss from both internal and external causes, e.g., theft by employees or third parties, cyberattacks, unauthorized access and mistakes. Mitsui also provides “individual consulting” to insureds to help insureds maintain appropriate security measures. Mitsui’s policy was developed with Japan’s largest bitcoin exchange, bitFlyer, which now ranks as the sixth-highest-by-volume bitcoin exchange in the world. This marks Japan’s continued endorsement of bitcoin and cryptocurrency; in April, the country began to accept bitcoin as a legal payment method.

Cryptocurrency appears to be here to stay, at least for the immediate future, and so do the risks associated with it. Companies dealing frequently in cryptocurrency would do well to consider obtaining an insurance product, like one discussed here, rather than hoping that coverage can be found in one of their existing insurance policies. As the use of cryptocurrencies becomes more widespread, companies may begin to consider using these products, even if they do not consider themselves to be primarily tech companies, as any new wave of technology has the potential to cause ripple effects throughout multiple industries.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Insurance Coverage for a Connected Technical World

By Perkins Coie on November 7, 2017

Some estimates calculate that over 23 ***billion*** "things" were connected through the internet in 2016. This number is projected to rise to over 50 billion by 2020. The broad category is known as the Internet of Things (IoT), and the new technology connects everything, from household devices to cars to industrial machinery, to the internet via enhanced sensors. The exponential growth in connectivity and new product development carry additional risks for companies investing in IoT technology. We offer some ways to protect your interests.

Consider the following examples:

- Smart phones controlling household items like security alarms
- Wearable devices monitoring fitness or health data
- Toys that interact with users via internet links
- Smart refrigerators, which order food necessities automatically when supplies are low
- Applications on your mobile device that track other's whereabouts
- Smart TVs
- Smart cars that monitor outside conditions and also automatically control when repairs are needed
- Homes that regulate lighting, temperatures and energy usage
- Industrial applications

What happens if a device malfunctions, resulting in property damage or injury to others? Devices that are linked to the internet can also be hacked. For example, some have speculated that the data breach at Target in 2014, which exposed personal information relating to approximately 70

million customers, was a result of hackers that gained access through inadequate security around the Target HVAC systems.

To the extent there are physical harms, data breaches or privacy issues, liability might affect businesses at any point in the production chain, including manufacturers, network providers and software developers. Careful attention to indemnification language in vendor agreements is one wat to help minimize the risks. Another is to closely examine your company's insurance portfolio to make sure that your insurance policies are as dynamic as your technology.

Even though insurance companies continue to tweak their forms to address new circumstances, the risks posed by Internet of Things technology may not fall neatly into any of your conventional insurance policy buckets. General liability insurance covers property damage and bodily injury but many policies now contain a broad electronic data exclusion. Some of the standard exclusions in general liability insurance policies – like the impaired property exclusion – can also severely limit coverage in situations where one product is used as a component in a larger product that later becomes damaged. There is also a risk that insurers could take a hard line on whether products/completed operations coverage is applicable, if software engineers continue to develop updates for technical issues that users download routinely to their devices. General liability policies are also generally limited to damages that are tangible, and not to electronic or other types of harm that might be deemed intangible by a court.

Cyber insurance can fill in some of the gaps, particularly where there are intangible harms, like those arising from hacking, data security and breach of privacy. This protection is absolutely critical for risks arising from Internet of Things operations. Nevertheless, this does not fill all of the gaps, as cyber policies usually exclude bodily injury and property damage, and so they would not address some of the risks left by the general liability coverage. There might also be limitations on certain types of privacy claims, like the improper collection of confidential information.

The best way to protect against any remaining risks may be through professional liability insurance designed for technical operations, referred to as technology errors and omissions coverage, also known as Tech E&O. This coverage is typically offered on a claims-made basis, and can be tailored in many circumstances to address your unique business profile. The policies can also, for example, include provisions, covering liability assumed by a contract, which could be a critical protection for software developers.

The potential risks and liabilities in this area suggest that the best way to protect your business at this juncture is to maintain all three types of insurance coverage – general liability, cyber liability and Tech E&O – and to tailor such coverage where possible, with the assistance of your broker,

to minimize any gaps raised by the risks for your particular business. The insurance industry will hopefully begin to address the complexities in this area, and make hybrid insurance products more commonly available in the near future.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Are You Protected Against Privacy Claims?

By Perkins Coie on November 3, 2017

Consumer privacy actions continue to be a huge, costly risk for any business handling customer data over the internet. Lawsuits alleging improper collection of consumer data, such as zip codes or contacts, have become commonplace. Is your company at risk? We share several recent settlements and lawsuits highlighting the risks of privacy claims.

Neiman Marcus. In March 2017, retailer Neiman Marcus agreed to a proposed settlement to pay $1.6 million in a consumer class action filed in response to a 2013 data breach that allegedly compromised the credit card data of approximately 350,000 consumers. The class alleged that Neiman Marcus failed to protect consumers' privacy and further harmed consumers by waiting 28 days to inform them of the breach.

As part of the settlement, Neiman Marcus agreed to maintain certain data security measures, such as increased frequency and depth of cybersecurity reporting, the use of chip-based payment infrastructure in stores, and education and training of employees on privacy and data security matters. Neiman Marcus also agreed to appoint a chief information security officer and to create an information security organizational unit. Each affected class member who submits a valid claim is further entitled to receive up to $100. The settlement is currently awaiting approval. *Remijas, et al. v. The Neiman Marcus Group, LLC*, Case No. 1:14-cv-01735 (N.D. Ill.).

We-Vibe. Another March 2017 settlement considers privacy in the context of the Internet of Things. Adult toy device maker We-Vibe agreed to settle a class action for $3.75 million. The We-Vibe product operates through connections with users' smartphones via Bluetooth and allows users to communicate with each other through video chat and text messages and to control another user's We-Vibe remotely. Consumers alleged that We-Vibe violated their privacy by collecting data through its app without their knowledge or consent; indeed, consumers alleged that We-Vibe marketed that its app was "secure." In particular, consumers alleged that We-Vibe collected data on (1) the date and time of each use, (2) the vibration intensity level selected by

the user, (3) the vibration mode or pattern selected by the user, and (4) where available, the email address of consumers who registered with the app. The settlement obtained preliminary approval on March 14, 2017. *N.P. et al. v. Standard Innovation Corp.*, Case No. 1:16-cv-8655 (N.D. Ill.).

Mass Transit App. Even more recently, San Francisco's BART and a software developer—Elerts Corp.—were sued in a proposed class action in California federal court on May 22, 2017, for the alleged secret gathering of cellphone owners' personal data though a BART app designed to provide transit information. *Pamela Moreno, et al. v. San Francisco Bay Area Rapid Transit District, Elerts Corp.*, Case No. 17-cv-2911 (N.D. Cal.).

Privacy Claims and Insurance Coverage

These matters highlight the increasing need for every company handling consumer data to carefully examine whether it has insurance coverage protecting against privacy-type claims. To the extent the underlying privacy claims are in the form of a proposed class action, particularly if brought in California, the cost to defend against such allegations can be substantial.

There is potential coverage through general commercial liability insurance (such as CGL policies) as well as stand-alone cyberpolicies. If your business handles consumer data, you may want to review existing policies or provisions in contemplated policies for such coverage. Many CGL policies, for example, contain broad exclusions purporting to eliminate any coverage relating to claims alleging the violation of "any" statute. While the courts are still testing the extent to which such exclusions cut off coverage, such broad exclusions may be argued by insurers to eliminate coverage for a wide array of privacy claims that flow from federal or state statutes. Similarly, your cyber policy might contain an unreasonably short "retroactive date," leading to potential arguments that such provisions eliminate coverage for many class actions that might relate to alleged privacy violations allegedly continuing for a course of years, or your policy might narrowly define the type of "personal information" that is covered or the circumstance of its release, leading to arguments that certain claims are not covered.

With privacy class actions remaining as popular claims, it may be appropriate for your company to reconsider whether it has appropriate coverage and whether any additional coverage should be obtained. Having appropriate coverage may mean the difference between a class action being merely a headache and being truly detrimental.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Cyber-Policy Coverage for Payment Card Industry (PCI) Fees

By Perkins Coie on November 3, 2017

Even though cyber breaches—hacks, ransomware attacks, denial or delay of service attacks, malware, phishing and the like— have existed for years, coverage under actual cyber policies (as opposed to CGL, D&O, or crime policies) is now starting to be litigated. One of the early issues that has been addressed under a cyber policy is if cyber policies provide coverage for Payment Card Industry (PCI) fees assessed by credit card companies in case of a data breach for which the insured is ultimately liable. In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 26, 2016), the court answered that question in the negative under the cyber policy at issue there.

The relevant facts will sound familiar to any retailer or restaurateur who has experienced a data breach. As P.F. Chang's (Chang's) allowed its customers to pay for their meals with credit cards, it had, as is standard practice under the circumstances, entered into a Master Service Agreement (the Agreement) with Bank of America Merchant Services (BAMS) under which BAMS processed credit card transactions for Chang's (essentially, BAMS functioned as an intermediary between Chang's and, as relevant here, MasterCard).

The Agreement incorporated MasterCard's PCI rules, which provided, among other things, that MasterCard could assess fees against BAMS if MasterCard experienced losses resulting from a data breach at a client of BAMS, such as Chang's. The Agreement also contained an indemnification clause under which Chang's agreed to indemnify BAMS for any such fees assessed against it because of a breach at Chang's. All of that is standard and well known in the industry and to insurers working with retailers and restaurants.

Chang's Hack and the Aftermath

Chang's was subsequently hacked, and the hackers posted on the internet the credit card numbers belonging to over 60,000 of Chang's customers. As a result, MasterCard incurred costs in fraudulent charges on its customers' credit cards as well as for the processes of notifying its customers of the potential that their credit cards were compromised and of providing them with new credit cards and pins, and the like.

MasterCard consequently assessed about $1.72 million in fees against BAMS (the PCI Fees), of which $1.7 million was for fraudulent charges and about $200,000 for the issuance of new credit cards and associated operational costs. BAMS sought indemnification from Chang's. Since BAMS would have stopped providing credit card processing services to Chang's had Chang's not paid, Chang's indemnified BAMS. Chang's then brought a claim against Federal Insurance Company (Federal) seeking reimbursement for the PCI Fees under Chang's cyber coverage with Federal. Federal denied the claim, and litigation ensued.

The district court initially found that there was no coverage in any event for the $1.7 million in fees for fraudulent charges because the policy provided that coverage was available only if the person making the claim against the insured was the person whose confidential records had been disclosed ("injury sustained . . . by a Person because of . . . unauthorized access to **such Person's** Record" (emphasis added)). Although BAMS had made the claim against Chang's when it sought indemnification for the $1.7 million, the records that had been disclosed did not belong to BAMS, they belonged to MasterCard. As such, there was no covered claim for the fees related to fraudulent charges. And although the court found that there was at least potential coverage for the remaining approximately $200,000 in PCI Fees, it also found that those fees fell under a policy exclusion "for contractual obligations an insured assumes with a third-party outside of the Policy."

In reaching this conclusion, the court held that Chang's had voluntarily entered into the Agreement with BAMS and had voluntarily agreed to indemnify BAMS. Moreover, there was no evidence that Chang's would have had to indemnify BAMS even if Chang's had not entered into the Agreement. Rather, to the contrary, Chang's had the duty to indemnify only because of the Agreement. The court was not swayed by Chang's argument that it had no choice but to enter into the Agreement if it wanted to allow its customers to pay by credit card. Similarly, the fact that Federal knew just as well as Chang's did that the assessment of PCI Fees and indemnification of credit card processing services by businesses accepting credit cards was standard practice in the industry was of no relevance to the court. To the contrary, the court said that since both Federal and Chang's were sophisticated parties, it assumed that they had contracted to have covered precisely what they wanted, which, under the facts and the plain language of the policy, clearly excluded the PCI Fees. Had Chang's wanted to have such fees covered, it should have

specifically asked for that—for example, through an exception to the contractually assumed-liability exclusion.

But there was no evidence that Chang's had sought to negotiate for coverage of PCI Fees, or that it had, at any time during the underwriting process, assumed or expected that such fees would be covered. Consequently, Chang's was simply out of luck.

Lessons Learned from *Chang's v. Federal*

As one would expect, Chang's appealed to the U.S. Court of Appeals for the Ninth Circuit, but the parties settled during the pendency of the appeal, and the appeal was dismissed. That means that the district court opinion discussed above is, at least for now, the last word of a court on the issues between Chang's and Federal. What's the significance? It means that, if you are a business that accepts credit cards as payment and contracts with a credit card processing service, you should:

1. confirm whether your credit card processing agreement contains a clause obliging you to indemnify the service provider for PCI fees (which it probably does);
2. review your cyber policy for a "contractually assumed liability" exclusion;
3. if there is such an exclusion, seek to negotiate an exception to it for PCI fees; and
4. beware of a definition of a "claim" as an injury sustained only by the person whose confidential records were harmed (i.e., beware of the "**such** person" language), and seek to have such language changed, or an endorsement added that specifically provides coverage for PCI fees, including fees for fraudulent credit card charges.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Ninth Circuit Weighs in on Coverage for Third-Party Claims Alleging Non-Fax-Related TCPA Violations

By Perkins Coie on October 28, 2017

The U.S. Court of Appeals for the Ninth Circuit **ruled in the negative** last month on whether **the Los Angeles Lakers were entitled to coverage** under their Directors and Officers (D&O) policy (Policy) for costs relating to an underlying suit brought against them alleging violations of the Telephone Consumer Protection Act (TCPA). Los Angeles Lakers, Inc. v. Federal Ins. Co., No. 15-55777 (9th Cir. Aug. 23, 2017). On its face, the ruling is favorable to insurers. But given the disparities between the opinions, its ultimate effect is unclear and will be revealed only in its future application.

The *Lakers* lead opinion adopted the Federal Insurance Company's (Federal's) broad argument that a TCPA claim is by definition a claim for invasion of privacy and therefore excluded from coverage under the Policy's broad exclusion from coverage of claims "based upon, arising from, or in consequence of . . . invasions of privacy" (Privacy Exclusion). *Id.* at 8-9. To reach its conclusion regarding the nature of TCPA claims, the lead opinion determined that the U.S. Congress enacted the TCPA with the express intent to protect privacy interests so that, "in pleading the elements of a TCPA claim, a plaintiff pleads an invasion of privacy claim." *Id.* at 14. That, combined with the very broad meaning the lead opinion gave to the Privacy Exclusion, meant that the Lakers were not entitled to coverage under the Policy.

The lead opinion's conclusion was joined by a short concurrence that would have upheld the district court decision on much narrower grounds. According to the concurrence, the underlying complaint alleged claims for invasion of privacy because it "alleged several times . . . that the message [the plaintiff] received [from the Lakers] was an invasion of his privacy." *Id.* at 20 (Murphy, III, J., concurring). That the specific claims at issue were ones for invasion of privacy was enough to deny coverage under the Policy, without "need[ing] to hold more broadly that a TCPA claim is inherently an invasion of privacy claim." *Id.* at 21.

Finally, there was dissent that would have overturned the district court decision and found that there was coverage under the Policy. To reach that conclusion, the dissent reasoned that the analysis had to start with the unambiguous language of the TCPA setting forth the elements of the underlying TCPA claim, which unambiguously does not require any allegation of invasion of privacy. *Id.* at 24 (Tallman, J., dissenting). The dissent found that dispositive to establish that TCPA claims are **not** per se claims for invasion of privacy—and since the statutory language was unambiguous, the dissent found no need to consider congressional intent. *Id.* at 22-24. But, in any event, in enacting the TCPA, Congress had also intended to "address[] public safety concerns, provide[] redress for economic injury, and protect[] *businesses* from ATDS calls." *Id.* at 25 (emphasis added). The latter intent, in particular, showed that TCPA claims are not inherently claims for invasion of privacy because "most states [including California] hold that business entities lack privacy interests" and therefore cannot bring invasion of privacy claims. *Id.* at 27 (internal alteration & quotation marks omitted).

Finally, the dissent concluded that the underlying claims in this particular case were not based on invasion of privacy because the TCPA plaintiff "did not seek recovery based on invasion of privacy" and "expressly disavowed all claims based on invasion of privacy" by seeking "only damages and injunctive relief for recovery of economic injury" (invasion of privacy is a personal, not an economic, injury). *Id.* at 29-31. On these bases, the dissent would have reversed the district court's dismissal of the Laker's claims against Federal.

What does that all mean? At first blush, the ruling is favorable to insurers and makes it more difficult for policyholders to get coverage for third-party TCPA claims under D&O policies. That is so because of the breadth of the lead opinion, both in characterizing TCPA claims and in construing the policy's privacy exclusion.

But the ruling is very divided, and even the lead opinion leaves room for further argument. For example, the lead opinion arguably overstates the breadth of the Privacy Exclusion by finding that it applied because the underlying claim "is unquestionably, at the very least, connected to an alleged invasion of privacy." *Id.*at 17. The exclusion, however, seems to require more than a "connection;" it seems to require some form of causation. *See id.* at 9. Moreover, the concurring opinion agreed with the lead opinion only to the extent that **the underlying claims in this particular case** were ones for invasion of privacy—it would not have gone so far as to characterize every single conceivable TCPA claim as such. And the dissent went even further to find that TCPA claims **cannot** be categorically characterized as ones for invasion of privacy.

Ultimately, only time will tell how broadly the lead opinion in this case will be applied.[1] In the meantime, in cases seeking coverage for TCPA claims under any policy with a broad privacy

exclusion, courts will almost certainly scrutinize the specific TCPA claims at issue to assess their connection to privacy-related claims. Despite its apparent breadth, the *Lakers* opinion does not seem to foreclose arguments that (1) the specific TCPA claims at issue are not privacy-related; (2) the privacy exclusion at issue is not as broad as stated in the lead opinion (or the lead opinion overstated the breadth of the exclusion); and (3) not all TCPA claims are ones for invasion of privacy.

Endnotes

[1] It is also possible that the Ninth Circuit itself will clarify or modify these decisions. On September 6, 2017, the Lakers sought *en banc* review of the panel opinions, and on September 8, 2017, the panel ordered Federal to respond to the Lakers' request by September 29, 2017. *See***https://www.law360.com/cases/555f06b3cc4ad17bf0000016/dockets**. Moreover, on September 18, 2017, the United Policyholders filed an *amicus curiae* brief in support of the Lakers' request for *en banc* review, arguing that the panel's lead opinion is "unmoored from the fundamental principles of insurance law that protect all insurance consumers" and contrary to the California Supreme Court's rules of construction for insurance policies. **Brief in Support of Petition for Rehearing En Banc on Behalf of Amicus Curiae United Policyholders**, at 2-3 (9th Cir. Sept. 18, 2017). So—stay tuned!

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Autonomous Vehicles: New Risks in A Driverless World

By Perkins Coie on October 21, 2017

Does your business manufacture autonomous vehicles, supply components or software for use in autonomous vehicles, or otherwise incorporate autonomous vehicles into its business plan? For any venture involving autonomous vehicles, there are new risks that your business should understand and insure.

But first, what exactly qualifies as an autonomous vehicle? There are varying levels of automation, and before evaluating insurance options, it is important to understand the levels of automation. The Society of Automotive Engineers (SAE) has established levels of automation on a scale of 0 to 5, from no automation to full automation, respectively. The **full chart created by SAE in its standard J3016 is available here.**

Coverage for Manufacturers of Autonomous Vehicles or Suppliers of Components or Software for Autonomous Vehicles

As automated vehicles move from Levels 0−2 to Levels 3−5, vehicles will have more control and responsibility for monitoring the driving environment. Accordingly, accidents caused by human error will start to decrease, and lawsuits against autonomous vehicle manufacturers and suppliers of autonomous vehicle components and software will increase.

Such a lawsuit might claim that a defect in the autonomous vehicle or in a particular component or software caused the accident. To protect your business, you should examine your Commercial General Liability (“CGL”) policy to ensure that it provides adequate coverage, if at all, for product liability claims. As a supplier, your business might additionally be at risk for a lawsuit from a manufacturer seeking indemnification if it is possible that a component or software that you supplied caused the accident.

In the hopefully unlikely event that your business might want to preempt any product liability claims by recalling an autonomous vehicle, component, or software, you should ensure that you

also have Product Recall coverage. CGL policies typically do not cover the expenses involved in a product recall. Suppliers should additionally ensure that they have both first-party and third-party product recall coverage to protect against any claims from buyers alleging that they have suffered damages as a result of a recall.

Coverage for Businesses Using Autonomous Vehicles

If your business uses autonomous vehicles, you should ensure that you have coverage beyond the standard automotive insurance policy. One of the first insurers to provide coverage for the owners of autonomous vehicles was Adrian Flux in the United Kingdom. Take a look at what its policy covers here. Generally, autonomous vehicle insurance should cover accidents caused by a vehicle sensor being blocked or covered up by mud or other debris, satellite outages, or a failure to timely update the vehicle's software.

Policies should also cover accidents with more malicious causes such as hacking. Businesses should be prepared for any potential hacks of their autonomous vehicles with cybersecurity insurance, and should examine their policy to ensure that it would provide coverage in the event of: hijacking of vehicle controls, ransomware, remote vehicle theft, unauthorized entry, identity theft, privacy breaches, and the theft or misuse of personal data.

Depending on how integral autonomous vehicles are to your business, it might be a good idea to examine whether your business has adequate Business Interruption insurance. For example, if your business uses autonomous vehicles to deliver products, and all of your vehicles are hacked, that would deliver a serious blow to your business operations. If this is a possibility for your business, you should examine your policies or consult with an insurance recovery attorney to ensure that such a scenario would be covered.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Is There Insurance Coverage for Virtual Currencies?

By Perkins Coie on October 16, 2017

Ever since the introduction of bitcoin in 2009, cryptocurrencies have become increasingly relevant to business transactions over the internet. Blockchain technology does afford additional protections to businesses using cryptocurrencies, but bitcoin, Ethereum and other cryptocurrencies represent value, and are at risk of loss, just like any other currency or asset. Insurers are in the formative stages of addressing these emerging risks, but there are still avenues, as well as new insurance products, to protect your virtual assets.

Bitcoin is an open source public payment system operating over the internet. It was designed to bypass the central bank model by using peer-to-peer technology. [For more information about bitcoin and blockchain technology, see "**Treatment of Bitcoin Under U.S. Property Law**."] Use of cryptocurrency involves what is known as public key cryptography, which uses digital signatures to secure information. Basically, the signatures consist of a public key (known to everyone) and a private key known only by the cryptocurrency owner. The private key is required to access and use the cryptocurrency. As such, the protection of those private keys is critical. Such keys can be lost or stolen. Is there coverage in the event of an inadvertent loss, a mistake or a hacking incident?

To the extent cryptocurrencies like bitcoin are characterized as the equivalent of money or securities (e.g., by a court or regulatory authority), then traditional forms of insurance coverage—like D&O, cyber, E&O and commercial crime insurance—should respond to losses faced by those owning and using cryptocurrency in their transactions.

But, given the conflicting views about how to characterize assets like bitcoin (e.g., currency vs. commodity), and because of the unique structure for owning and using such assets, there continues to be uncertainty about whether traditional forms of insurance will properly respond.

Here are some insurance-related suggestions for any business that plans to use cryptocurrency in its business:

- Make sure your cyber policy is broad enough to include triggering events that relate to bitcoin or other cryptocurrency transactions. For example, since the ownership and use of private keys is so central to bitcoin transactions, the definition of a claim event triggering the insurer's obligation to investigate, to fund remedial efforts, to provide notice to affected persons and to defend against claims must be broad enough to include the disclosure of confidential private key information or damage to the private key owner's security system.
- Commercial crime policies and financial institution bonds insure against the loss of assets caused by criminal or fraudulent activities, including employee dishonesty. At least one insurer has offered an endorsement to its policy that specifically includes "bitcoins" in the policy definition of "money." Also, check the causation requirements of the policy. To the extent coverage is limited to direct actions by third-party hackers, then your coverage may not respond to those situations—like a phishing attack—where a company employee is unknowingly controlled by an outside hacker. Bitpay's insurer denied coverage based on such a reading of a crime policy. *Bitpay v. Massachusetts Bay Ins. Co.*, Case No. 15-03238 (N.D. Ga.).
- It appears that bitcoin has become a favored currency for criminals responsible for ransomware, kidnaping and various forms of extortion. Kidnap and ransom insurance, as well as many cyber policies, provide indemnity for ransoms that must be paid to such extortionists. Check your policies to make sure that bitcoin is included as a currency subject to indemnification, and if possible, seek to include bitcoin expressly within the definition of money or currency.

As noted above, the insurance industry is responding to changes in the market by developing specialized products with cryptocurrency in mind. If your company is planning to provide bitcoin-related services or join the growing number of companies using cryptocurrency in its e-commerce, then you would be well-advised to consult with your broker about new professional liability, cyber and commercial crime policies that may be available.

At the very least, if your business could be using cryptocurrency in future transactions, you should carefully review traditional insurance provisions to determine whether definitions of things like "money" can be modified in your renewal or enhanced by an express endorsement.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

The Rising Independent Contractor Model and Protection Against Ensuing Misclassification Claims

By Perkins Coie on October 4, 2017

Most businesses, and startups in particular, need to keep costs down. Workers either cannot or do not want to work traditional hours. So begins the boom of the independent contractor model, or the so-called “1099 economy.” But when a startup wants to ensure consistency and quality and begins to exercise more control over a worker, it creates the potential for a misclassification lawsuit.

The line between an independent contractor and an employee is certainly not a bright line, and some may even argue the line is always moving. If a company utilizes the independent contractor model and exercises some control over its independent contractors, in light of the legal uncertainty, it would be prudent to have insurance coverage that would cover any misclassification claims.

As many as 84% of employment class action lawsuits are estimated to involve wage-and-hour claims, including misclassification. Instacart, for example, a mobile phone application which provides workers to shop for customers, is in the process of settling a class action lawsuit filed against it in Los Angeles Superior Court. *Casey Camp, et al. v. MapleBear, Inc. dba Instacart*, Case No. BC652216 (Calif. Super. Ct. Los Angeles Cnty.). The parties requested approval in April 2017 of a proposed $4.6 million settlement.

EPLI Coverage Tips

Wage-and-hour claims are typically excluded from Employment Practices Liability Insurance (EPLI) policies, but there are still ways to protect your business if you are looking to renew your insurance and also potential avenues of coverage for some claims if you are faced with a lawsuit. Here are some coverage tips to consider:

1. Some EPLI policies will in fact provide for the payment of defense costs relating to wage-and-hour claims (sometimes by special endorsement). This is something to consider requesting, particularly if you have significant operations in California.
2. Many employment claims allege multiple labor code violations, including, for example, failure to provide adequate rest breaks or failure to pay overtime wages. Many older EPLI policies purport to exclude claims arising from the Federal Labor Standards Act "or similar provisions of any federal, state or local statutory law or common law." Several California courts have held that causes of action for Labor Code Section 226 (failure to provide itemized wage statements to employees) are not similar to the FLSA, and thus are outside the FLSA exclusion. E.g., *PHP Ins. Service v. Greenwich Ins. Co.*, 2015 U.S. Dist. LEXIS 106274 (N.D. Cal. Aug. 12, 2015); *California Dairies, Inc. v. RSUI Indemnity Co.*, 617 F. Supp. 2d 1023 (E.D. Cal. 2009).
3. If an employment claim against you based on alleged wage-and-hour violations also includes causes of action for retaliation and/or misrepresentation, there might be an independent basis for coverage under your EPLI policy. In California and many other states, if any claim is potentially covered, the insurer must defend the entire action.
4. Recent amendments to Labor Code Section 558.1 make individuals potentially liable for the wage-and-hour violations of the employer company. Some D&O policies apply the wage-and-hour exclusion to claims against the company but do not necessarily apply to claims against an officer or other individual.

Careful review of all EPLI and D&O policies is therefore essential whenever a business faces adverse wage-and-hour claims, particularly those that allege a wide array of purported labor code violations.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Websites and Applications: A New Platform for ADA Claims

By Perkins Coie on September 28, 2017

In a world where brick-and-mortar businesses are traded in for an online presence, the realm of accessibility challenges is continually evolving. Your company needs to change the way they think about accessibility, including whether your current insurance covers ADA claims. It's time to start considering questions like: Are your websites and applications compatible with screen readers and other assistive technologies? Are your videos captioned?

Making websites and applications more accessible will be a benefit not only to those with disabilities, but also to other users. For example, cleaning up crowded pages with too much content makes it easier for screen-reading technology to adequately convey information and also generally improves readability for everyone.

The DOJ plans to release guidelines on online accessibility in 2018. In the meantime, companies should review and implement the **Web Content Accessibility Guidelines 2.0** (WCAG) published by the World Wide Web Consortium.

Insurance and ADA Claims

In 2016, over 250 ADA lawsuits were filed related to the accessibility of a website or application. Because the digital world is an ever-changing landscape, companies should be sure that their insurance policies cover ADA claims. Some policies might only cover portions of an ADA claim, such as defense costs, while excluding remediation costs. As always, it is important to examine the language of your policies and know what exactly is included and excluded from coverage.

Employment Practices Liability Insurance (EPLI) typically covers claims by an employee, but may not cover ADA claims brought by a customer. However, third-party EPLI coverage is built into many EPLI policies and can cover ADA claims brought by a customer. It is worth examining your

EPLI insurance before your next renewal, particularly if you have significant operations in California, where federal ADA and equivalent state statutory claims are routinely filed.

Another limitation to watch out for is your policy's definition of "claim." If the policy defines a claim as a "demand for monetary damages," that could pose a problem when trying to obtain coverage in a case where a person is requesting reasonable accommodations and not money damages.

Defending an ADA claim, particularly in the context of proposed class action claims, can be the most costly part of the battle, and where a business needs support from its insurer the most. Here again is where it pays to review your policy before renewal to make sure it is implicated by demands for both monetary and non-monetary relief. Under those circumstances, there is a better chance for coverage of not only your defense costs, but also of any attorneys' fees you must pay to the other side, even though there generally will not be coverage for the costs required to make your website and/or customer interface ADA-compliant.

If the ADA claim arises from a company's website, there is also potential for at least some recovery under a company's media liability insurance. While many media policies exclude discrimination claims (thus barring ADA causes of action), other media policies contain narrower exclusions, limited to only employment-related discrimination. This would allow recovery for ADA claims brought on the basis of the accessibility of a website.

In light of the high risks facing businesses in California, where plaintiffs are testing new grounds for accessibility allegations, as well as elsewhere, you would be well-served to do at least two things to protect your business: (1) check your EPLI and media policies before renewal to confirm that they are broad enough to address the defense of ADA claims, and (2) if you are on the receiving end of an allegation, check your EPLI and media policies thoroughly, and tender the claim if there is any possibility of coverage.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Key Language for Your D&O Policy

By Perkins Coie on September 20, 2017

Directors' and Officers' liability (D&O) coverage is important for any organization as it provides coverage for directors and officers who may be personally liable for suits brought against the company. However, all D&O policies are not created equal. Paying attention to nuances in your D&O policy when placing or renewing coverage can have huge implications if a claim is later brought against directors, officers or the company.

All D&O policies contain exclusions that deny coverage for liability arising from bad acts of the insured such as fraud, dishonesty, criminal acts or intentional misconduct. These exclusions are often invoked by insurers when directors and officers are charged with claims alleging fraud and self-dealing, sometimes prohibiting coverage. Insurance policies with these "bad act" exclusions frequently contain final adjudication language, meaning that the exclusions are only triggered if there is an actual finding of the bad act by either the trial court or by a court in separate coverage litigation. Ensuring that this final adjudication language is in your policy will prevent you from forfeiting your right to millions in potential coverage. Without final adjudication language, an insurer could disclaim coverage for a settlement if the underlying complaint alleged fraudulent conduct.

The importance of final adjudication language was underscored in a recent California case. In ***Stein v. Axis Insurance Co.***, 10 Cal. App. 5th 673, 216 Cal. Rptr. 3d 804 (2017), *as modified* (Apr. 6, 2017), the court held that the policy's "final adjudication" language required the insured to obtain a final *judgment* after appeal before the insurer was able to disclaim coverage, in spite of a jury's conviction of the insured for securities fraud.

Similarly important and often ignored during policy placement is the wording of severability clauses in D&O policies.

Severability provisions can preserve coverage for non-bad actor insureds in the event that other directors or officers are charged with acts that would eliminate coverage. Severability provisions

in D&O coverage can also ensure that if one insured makes a misrepresentation on the insurance application, which would be a bar to coverage and potentially give an insurer the right to rescind the policy, the coverage is not voided for all of the other covered directors and officers. The U.S. Court of Appeals for the Ninth Circuit (interpreting California law) upheld the rescission of a D&O policy for all insureds because the policy failed to contain a severability provision. *Fed. Ins. Co. v. Homestore, Inc.*, 144 F. App'x 641 (9th Cir. 2005). The policy stated that, in the event of a misrepresentation, the policy was "void and of no effect whatsoever" if the misrepresentation was known to be untrue on the inception date of the policy by one or more people who signed the application; policy rescinded for all insureds regardless of their knowledge of misrepresentation.

Another source of potential coverage disputes occurs when a claim is brought against the company (and/or a director and officer) and the claimant happens to also be an insured under the policy. This could happen in the context of a whistleblower, an employment claim or a claim in bankruptcy proceedings. These disputes can be extremely contentious and represent the type of claim for which your company would expect protection from its D&O insurer. Most D&O policies, however, contain a so-called "insured vs. insured" exclusion, which bars coverage for claims asserted by, or on behalf of, the insured against other parties insured by the policy. These provisions can and should be limited, so that they do not operate as a blanket bar to coverage. Checking to ensure that your policy's insured vs. insured exclusion carves back coverage for employment claims, whistleblower claims and bankruptcy proceedings will protect you in many claim situations. *See, e.g.*, *Hawker v. Doak*, No. 15-16013, 2017 WL 1147131 (9th Cir. Mar. 27, 2017), where insured vs. insured exclusion in a bank's insurance policy barred coverage for a claim brought by the FDIC in its capacity as a receiver of the insured bank.

These are just a handful of the types of D&O policy provisions that have far-reaching and tangible consequences when an insured seeks coverage. Carefully reviewing your policy and working with your insurer to craft endorsements that carve back coverage is essential to preserving coverage and ensuring that you (and your company) actually receive the coverage you believe you are getting.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Can Your Insurance Company Cancel Your Policy?

By Perkins Coie on September 15, 2017

In the fast-paced world of tech startups and business planning, you might not even consider whether your insurance policies could be yanked out from under you. After you have secured basic insurance to protect yourself and your assets against loss and liability, can your insurance company cancel your coverage at any time? Surprisingly, under some circumstances, the answer is yes. But you can protect against this with some advance preparation.

For some forms of insurance—like health, life, auto or homeowner's insurance—there are statutory limitations on an insurance company's right to cancel. But, it's a different story for commercial insurance, purchased to protect your business assets and executives.

In California (and various other states), the insurance company has a brief window of 60 days after a policy is issued to cancel the coverage. After 60 days, the general rule is that an insurance company cannot cancel coverage, except for non-payment of premium. *But, this can be changed by the insurance company by adding a provision to its policy permitting cancellation*.

For example, some policies contain the following provision:

We may cancel this policy by mailing or delivering to the first Named Insured written notice of cancellation at least 30 days before the effective date of cancellation.

You might not think to look at the fine print of your insurance policy until after you have tendered a claim and then received a cancellation notice from your insurer. Or, you might receive a notice of cancellation out of the blue without any warning. If the insurance company has inserted a provision like the one above in its policy, it is generally enforceable.

Here's what you can do to avoid such a situation:

1. Ask to see the policy form before you agree to pay for it (that is, before it is officially bound). Sometimes, you can request that cancellation provisions be removed or more narrowly limited to certain circumstances (like to a misrepresentation in your insurance application or a material change in your business).
2. If you have tendered a claim before receipt of the cancellation notice, you may be able to force the insurance company to pay for the claim. At the very least, you might be entitled to the return of some portion of the premium you paid.

Here's the bottom line: Check the proposed language of any policy you are about to purchase to see if the insurance company has reserved for itself the right to cancel coverage for any reason. If so, request that they limit cancellation to non-payment of premium alone. If they won't modify the policy, you might want to go with a different insurer.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Risks of Offering "Damage Protection" to Customers

By Perkins Coie on September 7, 2017

Does your business model include a "protection plan" for customers that pays them for damages caused by your services? This can be an attractive component of your business and a way to reassure your customers. The protection is typically an easy value add-on in the apps that customers access via the internet or mobile devices. But because your business is agreeing to indemnify against loss arising from a contingent or unknown future event, does that subject it to restrictions on selling insurance?

The regulation of insurance is done on a state-by-state basis, and different states have different definitions of when a business must obtain a license to sell "insurance."

In the context of storage businesses, the Supreme Court of California is currently reviewing whether a "customer goods protection plan" offered by a storage company to customers who want extra value protection for their personal property is subject to state licensing requirements. *See Heckart v. A-1 Self Storage,* Case No. S232322.

In *Heckart*, the California Court of Appeal (Fourth District) applied what is called the "principal object and purpose" test and held that the damage protection plan was not insurance. This is consistent with other cases in other business contexts. For example, in *Wayne v. DHL*, 2008 WL 2503245 (Cal. Ct. of Appeal, 2nd Dist., June 24, 2008) (unpublished), the court addressed whether DHL was improperly selling insurance when it offered customers so-called "shipment value protection" for packages being delivered by DHL. For a small fee, DHL would agree to pay a higher value to the customer if the property being delivered was damaged. Otherwise, DHL's liability was limited.

The court said this was not insurance for the following reasons:

- The protection plan was an option that the customer could voluntarily choose to purchase or not.

- The principal object and purpose of the transaction was transportation, not insurance.
- DHL was the sole insured on a policy of inland marine insurance—DHL's customers were not additional insureds under that policy.
- The insurer paid DHL—not the shipping customer—in the event of a loss.

Oral argument in *Heckart* is expected later this summer and the Court's decision will shed additional light on whether the "principal object and purpose" test applies broadly in California. If your business operates in other jurisdictions, a review of other state regulations might be advisable.

PERKINSCOIE
Tech Risk Report
PROTECTING INNOVATIVE COMPANIES AGAINST 21ST CENTURY RISKS

Tips on Drafting Vendor Contracts

By Perkins Coie on September 1, 2017

If your company uses vendors, you're likely already familiar with vendor contracts. General provisions in the contracts, such as timing and delivery requirements, are well known, but did you know that inadequate insurance requirements in vendor contracts could put your company at risk? Learn the important, but frequently missed, insurance provisions that should be in all vendor contracts.

Your vendor contracts should clearly state the types of insurance your vendors must obtain before doing work with your company, including the minimum limits of liability that you expect the vendors to carry. Common types of insurance required of vendors are Commercial General Liability (CGL) insurance, Cyber Risk insurance, Professional Liability/Errors and Omissions (E&O) insurance, Automobile Liability insurance and Workers' Compensation insurance.

CGL insurance. This will provide coverage for the vendor in the event that an accident involves its premises, operations and/or products. Be sure to require that the vendor's CGL policy does not restrict coverage based on contractual liability; if it does and your company is not named as an additional insured (see below), you may be without coverage despite your contractual agreement with the vendor. CGL policies frequently provide insurers with rights of subrogation. In the event, however, that your vendor harms a person or property while delivering your products, it is possible that the vendor's insurer could attempt to sue your company to recover amounts paid on the claim! Requiring a waiver of subrogation from your vendor's insurer will prevent your company from becoming entangled in unanticipated litigation.

Cyber Risk insurance. If your vendor will be using, storing or accessing any private, confidential or protected information, be sure to require that it maintain Cyber Risk insurance. Cyber Risk insurance will ensure that your vendor is covered in the event of a data breach, which is essential. Click **here** for more information about cyber insurance.

Professional Liability/E&O insurance. Depending on the types of vendor services your company employs, you may want to require the vendor to maintain Professional Liability or E&O coverage. This coverage protects the vendor from errors in the performance of professional duties, such as software design, development and implementation. Think carefully if your vendor's negligence in providing services could result in financial losses for your company. If it could, you may want to require that the vendor purchase E&O insurance.

Automobile Liability and Workers' Compensation insurance. While often thought of as secondary, Automobile Liability and Workers' Compensation insurance coverages are essential. They aim to protect your company by ensuring that the vendor is adequately insured in the event any accidents occur when goods or services are being delivered to you.

Additional Insured insurance. When working with vendors, you should not only double-check that the vendor has maintained sufficient levels and types of insurance, but also consider being included as an Additional Insured on the vendor's policies. Additional insured provisions take many forms, and you should speak with your insurance broker or coverage counsel before deciding which is best for your company. In theory, being included as an additional insured provides protection as if your company was a named insured on the vendor's policy. However, some additional insured endorsements limit coverage to certain loss amounts or to certain activities and products. You should remember to review the additional insured provision in advance to make sure that you are getting the broadest protection and to prevent surprises later in the event of a claim.

It is not unusual for some vendor contracts to require the purchaser of services or goods (that is, you) to add the vendor as an additional insured to the purchaser's policy. If your contract requires such an addition, be sure that you work with your insurer to properly add the additional insured vendor as required by the terms of the vendor contract.

Certificate of insurance. Perhaps the most important aspect of insurance coverage in vendor contracts involves the requirement that the vendor provide you with a certificate of insurance. A certificate of insurance should evidence that the vendor in fact has obtained all of the insurance required in the vendor contract. Many contracts contain the requirement of furnishing a certificate of insurance, but all too often companies do not actually follow up to receive the certificate until a problem occurs. Designate an individual in your company familiar with insurance to be responsible for receiving the certificates of insurance and reviewing them to ensure that all of your company's requirements are actually met.

Note, however, that a certificate of insurance is not itself insurance. If there is a claim against you, there is no guarantee that you are protected by the vendor's insurance, even if you have a certificate of insurance. In your vendor agreements, you should require the vendor to provide, at the very least, 60 days' notice before the vendor can cancel its insurance. You can also reserve for yourself the right to request and review the insurance policies the vendor is required to maintain. And at the very least, you should request that additional insured endorsements accompany any certificate of insurance the vendor is required to provide.

Taking proactive steps to ensure that the insurance requirements in your vendor contracts accurately reflect the needs of your company is vital to avoiding complicated insurance issues when claims arise. If you are unsure what types of risks might be applicable to your company's various vendor contracts, be sure to work with a professional who can adequately identify potential liability issues and ensure your company is protected.

This update was republished on September 12, 2017 by *Law360*, "**Insurance Considerations For Drafting Vendor Contracts**".

Impairment Of Computer Services — Malicious Programming

Coverages

Impairment Of Computer Services - Inside Attack

We will pay for the actual:

- **electronic data recovery costs;**
- **business income** loss; and
- **extra expense,**

you incur due to the actual impairment of your **operations** during the **period of recovery of computer service,** not to exceed the applicable Limit Of Insurance for Impairment Of Computer Services - Inside Attack shown in the Declarations.

This actual impairment of **operations** must be caused by or result from actual loss to **electronic data** or a **system** due to **malicious programming** by an **insider,** unless an exclusion applies.

Impairment Of Computer Services - Outside Attack

We will pay for the actual:

- **electronic data recovery costs;**
- **business income** loss; and
- **extra expense,**

you incur due to the actual impairment of your **operations** during the **period of recovery of computer service,** not to exceed the applicable Limit Of Insurance for Impairment Of Computer Services - Outside Attack shown in the Declarations.

This actual impairment of **operations** must be caused by or result from actual loss to **electronic data** or a **system** due to **malicious programming** by an **outsider,** unless an exclusion applies.

Policy Exclusions

The following Policy Exclusions apply to all coverages provided in this contract.

Dishonesty

This insurance does not apply to loss caused by or resulting from fraudulent, dishonest or criminal acts or omissions committed alone or in collusion with others by you, your partners, members, officers, managers, directors, trustees, employees, anyone performing acts coming within the scope of the usual duties of your employees, or by anyone authorized to act for you, or anyone to whom you have entrusted covered property for any purpose.

This Dishonesty exclusion does not apply to **malicious programming** by an **insider.**

Loss Determination
(continued)

Extra Expense

The amount of **extra expense** loss will be determined based on necessary expenses that:

- exceed your normal operating expenses that would have been incurred by **operations** during the **period of recovery of computer services**, if no **malicious programming** had occurred; and
- reduce the **business income** loss that otherwise would have been incurred.

We will deduct from the total of such expenses:

- the salvage value that remains of any property bought for temporary use during the **period of recovery of computer services**, once **operations** are resumed; and
- any **extra expense** that is paid for by other insurance.

Resumption Or Continuance Of Operations

We will reduce the amount of any **business income** loss payment to the extent you can resume or continue your **operations**, in whole or in part, by using any available **electronic data** or **system**, including the **electronic data** or **system** impacted by the **malicious programming**.

If you elect not to resume or continue **operations**:

- any loss determination for **business income** will be based on the length of time it would have taken to resume or continue **operations** with due diligence and dispatch; and
- we will not make any payment for **extra expense**.

Loss Payment Limitations

Contributing Physical Loss Or Damage

We will not pay for any **business income** loss or **extra expense** caused by or resulting from **malicious programming** if direct physical loss or damage:

- contributes concurrently to, or
- contributes in any sequence to,

such **business income** loss or **extra expense**.

Extortion

We will not pay that part of any **business income** loss or **extra expense** you incur to respond to extortion or other similar threat.

Loss Of Market

We will not pay for any loss that results from loss of market, loss of use or delay.

Impairment Of Computer Services — Malicious Programming

Additional Condition

System Security

If a **system** is protected by **security software**, you are required to maintain and, as necessary, upgrade (at your own cost) such software so that it provides a technologically credible level of security.

We will not pay for any loss caused by **malicious programming** if, prior to the **malicious programming**, you:

- knew of any defect or deficiency in the **security software** and failed to correct it;
- failed to maintain the **security software** in complete working order; or
- knew of any technologically credible upgrades to the **security software** that could have prevented the **malicious programming**, and failed to make them.

Amended Definition

Extra Expense

Extra expense means necessary expenses you incur in an attempt to continue **operations**, over and above the expenses you would have normally incurred.

Electronic Data Recovery Costs

Electronic data recovery costs means the reasonable and necessary costs you incur to:

- copy, re-create, replace or retrieve **electronic data** you own or use, or which resides on a system you own or lease; and
- restore a system you own or lease to the functionality that existed prior to the **malicious programming**.

Electronic data recovery costs does not include the cost to repair or replace **electronic data processing equipment** or **communication property** which suffers direct physical loss or damage.

Extra Expense

Extra expense means necessary expenses you incur:

A. in an attempt to continue **operations**, over and above the expenses you would have normally incurred; and

B. to repair or replace any **property**, or to research or restore the lost information on damaged **valuable papers**, records and media, if such action will reduce any loss we would pay under this insurance.

Paragraph B. does not apply to Fungus Clean-up Or Removal Premises Coverage.

Malicious Programming

Malicious programming means an illegal or malicious entry into **electronic data** or a **system** which results in functions that:

- distort;
- corrupt;
- manipulate;
- copy;
- delete;
- destroy;
- slow down; or
- prevent the use of,

such **electronic data** or **system**.

Malicious programming does not mean:

- theft of telephone services; or
- direct physical loss or damage to **electronic data processing property** or **mobile communication property**.

Period Of Recovery Of Computer Service

Period of recovery of computer service means the period of time that:

- for **electronic data recovery costs** and **extra expense**, begins immediately after the **malicious programming** occurs; and
- for **business income**, begins 24 consecutive hours after the **malicious programming** occurs.

Period of recovery of computer service will continue until the earlier of the following:

- the date your **operations** are restored, with due diligence and dispatch, to the condition that would have existed had there been no **malicious programming**; or

Security Software	**Security software** means software or other computer applicatio ns or programming principally designed to detect, prevent or mitigate **malicious programming**.

Coverage B – Destructive Programming Liability

THIS COVERAGE APPLIES ON A CLAIMS-MADE BASIS. SEE THE PROVISION TITLED CLAIMS-MADE LIABILITY COVERAGE COMMON PROVISIONS.

Subject to all of the terms and conditions of this insurance, we will pay damages and **claimant costs** that the **insured** becomes legally obligated to pay, including by reason of liability of another person or organization that you assume in an **indemnity contract**, for **financial injury** caused by an **act**:

- that is an actual or suspected failure to perform your obligations under a written contract or agreement that authorizes you to use another person's or organization's **information and network technology product**; and
- that results in **destructive programming**.

This coverage does not apply to any damages, loss, cost or expense arising out of any actual or suspected:

A. defect, deficiency, inadequacy or dangerous condition in:

1. **your product**; or
2. **your service**; or

B. failure:

1. of **your product** to perform; or
2. to perform **your service**;

in accordance with the terms of a contract or agreement.

Coverage C – Cyber Liability

THIS COVERAGE APPLIES ON A CLAIMS-MADE BASIS. SEE THE PROVISION TITLED CLAIMS-MADE LIABILITY COVERAGE COMMON PROVISIONS.

Subject to all of the terms and conditions of this insurance, we will pay damages and **claimant costs** that the **insured** becomes legally obligated to pay for injury caused by an **act** of **unauthorized access or use**.

This coverage does not apply to any damages, loss, cost or expense arising out of any actual or suspected:

A. defect, deficiency, inadequacy or dangerous condition in:

1. **your product**; or
2. **your service**; or

B. failure:

1. of **your product** to perform; or
2. to perform **your service**;

in accordance with the terms of a contract or agreement.

Further, this coverage does not apply to damages, loss, cost, or expense any **insured** becomes legally obligated to pay by reason of assumption of liability in a contract or agreement, unless such **insured** would be liable for such damages, loss, cost or expense in the absence of such contract or agreement.

Additional Coverages

These Additional Coverages apply only if a Limit Of Insurance for such Additional Coverages is shown in the Declarations.

Privacy Remediation Expenses

Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for **privacy remediation expenses**, paid or incurred by such **insured**, that result from actual or suspected injury, caused by an **act** that results in a **privacy data breach** that first occurs during the policy period.

If it cannot be determined when the **privacy data breach** first occurred, then such breach will be deemed to have first occurred at the time you first notify us in writing that you are required to incur "Notification Expenses".

This Additional Coverage applies only if:

- such actual or suspected injury is not excluded under any section of this contract; and
- expenses are reported to us in writing within one year of the date the **privacy data breach** first occurred.

This Additional Coverage does not apply to **privacy remediation expenses** the **insured** is obligated to incur pursuant to the terms of a written contract or agreement.

Our obligations hereunder end when we have used up the applicable Limits Of Insurance.

We have no other obligation or liability to pay sums or perform acts or services under this Additional Coverage.

Enhancement, Maintenance Or Prevention Expenses (Except Privacy Remediation Expenses)	This insurance does not apply to any cost or expense incurred by any **insured** or others for any: • enhancement or maintenance of any property; or • prevention of any injury to any person, property or organization. This exclusion does not apply to Privacy Remediation Expenses Additional Coverage.
Equitable Relief (Except Privacy Remediation Expenses)	This insurance does not apply to any cost or expense to comply with any injunction or other equitable relief. This exclusion does not apply to Privacy Remediation Expenses Additional Coverage.
Governmental Claims Or Proceedings	This insurance does not apply to any damages, loss, cost or expense in any way related to any claim made or proceeding brought by or on behalf of any governmental authority. This exclusion does not apply to: • the liability for damages for injury sustained by a governmental authority (other than the **insured**) resulting from its ownership, maintenance or use of **your product** or **your service**. • Privacy Remediation Expenses Additional Coverage.

Definitions
(continued)

Cyber-Threat Expense

Cyber-threat expense means:

A. property or other consideration surrendered to remove or mitigate a **threat**; or

B. reasonable and necessary expenses incurred for:

1. the services of an independent negotiator or consultant; and
2. travel and accommodation expenses;

solely and directly incurred as a result of a **threat**.

Destructive Programming

Destructive programming means programming that:

- copies;
- corrupts;
- deletes;
- destroys;
- discloses;
- distorts; or
- manipulates;

software, data or other information or slows down an **information and network technology product**.

The following exclusion is added to this policy and replaces any similar exclusion contained therein. The use of the words damages, loss, cost or expense in any exclusion does not expand any coverages under this contract.

Exclusion Endorsement

Information Laws, Including Unauthorized Or Unsolicited Communications

With respect to all coverages under this contract, this insurance does not apply to any damages, loss, cost or expense arising out of any actual or alleged or threatened violation of:

- the United States of America CAN-SPAM Act of 2003 (or any law amendatory thereof) or any similar regulatory or statutory law in any other jurisdiction.
- the United States of America Telephone Consumer Protection Act (TCPA) of 1991 (or any law amendatory thereof) or any similar regulatory or statutory law in any other jurisdiction.
- the United States of America Fair Credit Reporting Act (FCRA) (or any law amendatory thereof including the Fair and Accurate Credit Transactions Act (FACTA))or any similar regulatory or statutory law in any other jurisdiction.
- any other regulatory or statutory law in any jurisdiction that addresses, limits or prohibits the collecting, communicating, disposal, dissemination, distribution, monitoring, printing, publication, recording, sending or transmitting of content, information or material.

continued

Additional Coverages

Fines Or Penalties For Privacy Data Breach

Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for civil fines or civil penalties imposed against such **insured** by order of a regulatory authority having jurisdiction caused by an **act** that results in a **privacy data breach** that first occurs during the policy period.

This Additional Coverage applies only if:

- such actual or suspected injury is not excluded under any section of this contract; and
- such fines or penalties are reported to us in writing within 60 days of the date the fines or penalties are imposed.

Our obligations hereunder end when we have used up the applicable Limits Of Insurance.

We have no other obligation or liability to pay sums or perform acts or services under this Additional Coverage.

continued

Additional Coverages

Confidential Information Breach Expenses

Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for **confidential information breach expenses**, paid or incurred by such **insured**, that result from actual or suspected injury, caused by an **act** that results in **disclosure of confidential information** that first occurs during the policy period.

If it cannot be determined when the **disclosure of confidential information** first occurred, then such disclosure will be deemed to have first occurred at the time you are first notified of a violation of the expressed confidentiality or non-disclosure terms of a written contract or agreement pertaining to your business.

This Additional Coverage applies only if:

- such actual or suspected injury is not excluded under any section of this contract; and
- expenses are reported to us in writing within one year of the date the **disclosure of confidential information** first occurred.

This Additional Coverage does not apply to **confidential information breach expenses** the **insured** is obligated to incur pursuant to the terms of a written contract or agreement.

Our obligations hereunder end when we have used up the applicable Limits Of Insurance.

continued

Under Additional Coverages, the following Additional Coverage is added.

Additional Coverages

Misappropriation Of Communication Services

Subject to all of the terms and conditions of this insurance, we will reimburse the **first named insured** for:

- charges and expenses; and
- reasonable and necessary costs to mitigate such charges and expenses;

paid or incurred by such **insured** that result from fraudulent access or fraudulent use of **communication services**.

If it cannot be determined when such fraudulent access or fraudulent use first occurred, then the fraudulent access or fraudulent use will be deemed to have first occurred at the time you first notify us in writing of the fraudulent access or fraudulent use.

This Additional Coverage applies only if such charges, expenses or costs are:

- not excluded under any section of this contract; and
- reported to us in writing within one year of the date the fraudulent access or fraudulent use first occurred.

Our obligations hereunder end when we have used up the applicable Limits Of Insurance.

continued