

Cyber Liability: Data, Privacy and the Perils of Social Networking

What Exactly Is Cyber Liability?

Challenges of Cyber Liability

- Stupendous growth of electronic *data storage* and *communication* has created new challenges for business entities.
- These new challenges fall into two main categories:
 - 1) Claims based on an Insured's access to *private employee data*.
 - 2) *Data breach* claims based on lost or compromised data.

Claim Examples – Employee Privacy

- An employer uses “private” information obtained from a social networking site to make a decision about a potential employee.
- An employer accesses a social networking site to gain negative information about an employee, then firing the employee.
- An employer accesses an employee’s private e-mail account, using the information against the employee.
- An employer accesses an employee’s cell phone text messages, using the information against the employee.

Claim Examples – Data Breach

- Online retailer’s network is hacked and customer credit card information is stolen, resulting in a customer class action suit and regulatory investigations.
- Companies unknowingly spread a worm, virus or other corrupting file via email to third parties, facing liability from those parties based upon lost revenues caused by the virus.
- Company attempts to “clean” the hard drives of their discarded computers, but a hacker recovers the data, including customer financial information.
- Disgruntled employee deletes the company’s databases, causing business interruption
- Computer hacker floods a company’s website, overwhelming the system and causing it to crash.
- Employee takes home a laptop computer, which is stolen. The laptop contained customer credit card information, leading to claims for identity theft.
- Employee accesses private medical records and discloses sensitive information about another employee or customer to a third party, leading to a suit for defamation and invasion of privacy.

Claim Examples - Other

- Some claims do not fall neatly in the categories of “employee privacy” or “data breach,” and relate more to traditional causes of action through new mediums (such as defamation, copyright infringement, and patent infringement):
 - Online publisher allows defamatory postings about a local public figure, causing the public official to lose his job.
 - Company is sued for unauthorized use of a person’s photo on its website.
 - A small business creates a website and is sued by another company alleging that their domain name violated trademark laws.

Two Challenging Types of Claims

- Cyber-Privacy: Claims arising from a compromise of employee cyber-privacy
- Data Breach: Claims arising from a breach of company data (first and third-party)

Response by Insurance Carriers

- Carriers recognize that cyber-related claims require a new approach, including tailored policies and careful handling.
- Insurers are responding by creating new policies or endorsements to traditional policies to respond to cyber-privacy issues:
 - Enhanced Privacy Endorsements
 - Technology and Media Coverage add-ons
 - EPL enhancements

Employee Cyber-Privacy Claims

Employee-Related (Cyber Privacy) Claims

- Examples of cyber-privacy issues in the employment context include:
 - Employers using info from social networking sites
 - Employers accessing personal e-mail accounts used from the employers’ computers
 - Employers monitoring personal e-mail messages sent by employees
 - Employers accessing text messages on employer-provided phones

Liability Risks Posed by Social Networking

- **Traditional EPL Claims:** Title VII, ADA, ADEA Dispute Treatment Claims Arising from Inconsistent Application of Social Networking Policies
- **Newer EPL “Social Networking” Claims:** Defamation, Libel, Breach of Privacy, Tortious Interference
- Breach Of Contract
- Adverse Evidence At Trial
- Exposure Of E-Discovery Violations
- Negative Publicity & Embarrassment
- Increased Exposure For Punitive Damages Due To Perceived “Willful” or Intentional Tortious Conduct
- Potential Ethical Violations From Improper Use Of Social Networking

Hiring Issues

- Even before an individual is an employee, social networking sites can cause problems for an employer:
 - Common for employers to review information on social networking sites to evaluate applicants
 - Over 80% of employers do!
 - Generally, there is this is not a problem
 - However, employers may be exposed to liability depending on how the information is gathered and used

Discrimination Claims Arising from Using Social Networking Sites in Hiring

- An example of improper use comes from discrimination claims
 - It is fine for employers to gather information about behavior, falsifying credentials, or negative comments about past employers
 - However, applicants may reveal information about their age, religion, disability or other protected categories
 - If both types of information are contained on the same social networking site, the employer may face a claim of discrimination, when the hiring decision was actually made solely from non-protected information

Discrimination Claims – An Example

- A corporate recruiter visited a potential physician recruit’s Facebook page, and found pictures of the individual taking her shirt off. <http://www.msnbc.msn.com/id/20202935/>.
 - The recruiter turned the candidate down, saying that the pictures would hurt the reputation of the hospital.
- But what if that’s not all that was on the Facebook entry?
 - The candidate could have been lesbian, pregnant, Muslim, disabled, or even just ultra-conservative.
 - An employer cannot make a hiring decision based on any of the above factors, so must show that it made the decision solely on behavioral characteristics.
 - Finding and *acting on* the Facebook pictures can very easily be a double-edged sword.

Employee Cyber Claims

- The potential pitfalls of social networking sites and other electronic data only increase once an insured begins dealing with employees.
- Particularly, Insured employers need to know when, and if, they can access employee data or communications, and when potential liability arises.

Cyber Privacy - Considerations

- The ultimate analysis will center around whether the employee had a reasonable expectation of privacy regarding the data or communication.
- One consideration is the content of the internal policies provided by the insured employer to the employee.
 - The primary factors include whether the content, communication, and scope of the policy was adequate to grant a right of access.
- A second factor is the nature of the data in question.

Employers Want to Know What Their Employees are Saying . . .

- Even in the supposedly public forum of the internet, employers must use care in how they access information.
 - In *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002), a pilot maintained a private website where he criticized the employer.
 - A manager obtained the password from an employee who was a member of the website, and used information therein against the pilot.

Some Courts Allow an Employer’s Investigation

- In this case, the court found in favor of the airline.
 - The manager’s logging into the website was not an “interception” of communication under the Wiretap Act.
 - The employee authorized the manager to access the website, precluding any claim under the Stored Communications Act.
- But questions still remain based on jurisdiction and the means of access:
 - What if the manager used technological means to obtain the password...that might be an “interception.”
 - What if the manager coerced the employee to give him the log-in information? That might violate the SCA.
- However, the case law is unsettled, and employers must use care in what they access.

Some Courts Find the Employer Overstepped Its Bounds

- An opposite result was reached in *Pietrylo v. Hillstone Restaurant Group*, 2008 U.S. Dist. LEXIS 108834 (D.N.J. 2008)
 - The employer accessed a chat group on an employee’s MySpace account, without receiving any authorization from members of the group.
 - The jury upheld punitive damages against the employer under the SCA for firing the involved employees, based largely on the fact that the employer coerced an employee into providing log-in information.

The Contents of a Data/Communication Privacy Policy May Be the Key

- A well-worded and properly communicated privacy policy may prevent employee cyber-privacy claims.
 - In *The Guard Publishing Co.*, 351 N.L.R.B. 70 (Dec. 16, 2007), the company policy prohibited any “non job-related solicitations,” but was only acted on when an employee sent e-mails relating to union support (as opposed to purely personal messages).
 - The union filed a charge with NLRB, but the Board found in favor of the employee, holding that the policy was not discriminatory and that the employees had no statutory right to use the company’s e-mail system, despite NLRA rules regarding the right to assist labor organizations.

Privacy Policy Content

- As is often the case, laws exist as a guide what an Insured must do to protect its interests.
- For example, the Stored Communications Data Act is violated when:
 - An employer intentionally accesses an electronic communication without authorization; or
 - Intentionally exceeds its authorization to access the facility to obtain an electronic communication.

**Laws Affecting Privacy Policies -
Stored Communications Act (SCA)**

- While there are many avenues to liability for unwarranted access to employee data, the SCA is an example of one of the more dangerous. 18 U.S.C. § 2707.
- The SCA imposes liability for unauthorized, intentional access to a facility in which electronic communication service is provided.
- A classic example is an employer who accesses an employee private e-mail account.
- The SCA allows for statutory damages in the event any actual damages are proven.
- Of greater concern, the SCA also permits the imposition of punitive damages and shifting of attorneys' fees, even without actual damages. See *Van Alstyne v. Elec. Scriptorium Ltd.*, 560 F.3d 199 (4th Cir. 2009).
- Even where an insured's intentional act causes no actual harm, the potential liability is significant.

Privacy Policy Content

- Regardless of the medium, an employer's accessing "personal" data or communications comes down to one question:
 - Did the employee have a reasonable expectation of privacy?
 - This applies to both social networking sites and e-mail communications.
 - The Privacy Policy can easily guide this analysis.

**Cyber Privacy –
Privacy Policy Content**

- Was the content of the policy clear and appropriate?
 - The policy should specify that all communications (not just work-related communications) are owned or will be monitored by the Insured.
 - The policy should be clear on whether it applies to only work-provided e-mail accounts or all e-mail accounts.
 - The policy should specify the types and levels of employees to which it applies.

**Cyber Privacy –
Policy Communication**

- **How well was the policy communicated or enforced?**
 - The policy should have been drafted recently enough to apply to current technology.
 - The Insured should have kept employees apprised of all revisions.
 - Communication of the policy, ideally, would have been through employee training.
 - The Insured should have required the employee to sign off on an acceptance of the policy at the time of his or her hire, and when all subsequent versions of the policy were released.

**Cyber Privacy –
Nexus to Business Interest**

- **Did the policy have a reasonable relationship to a legitimate business interest of the insured?**
 - Even if the content and communication are sound, the policy must further a legitimate business interest of the Insured.
 - For example, courts have held that a company may not transform all private communications into company-owned communications only because the company provided the hardware: the actions of the employee must be in furtherance of a legitimate business interest.

**Cyber Privacy –
Use of Employee Data**

- **Was the employee data being used for a purpose that broadened the Insured’s right of access?**
 - Communications between and employee or his/her attorney will receive the highest level of protection.
 - Data that violates a law or clear workplace policy will usually be subject to greater control by the Insured (e.g., obscene, threatening, harassing or otherwise inappropriate material).
 - Any communication that relates directly to the Insured’s legitimate business interests will typically be subject to greater control by the Insured.

Cyber Privacy – Final Thoughts

- Sometimes, even things that look simple might not be...

Facebook Firing



Cyber Privacy – What Is Simple?

- Most employers would likely agree that the Facebook employee was rightly fired, with cause.
- However, they (and we) need to think about the response.
 - It was not necessary for the manager to respond in a public forum.
 - The mix of a public forum and use of profane, disparaging phrases could create liability, even though the employee “clearly” asked for it.
 - It is never again going to be simple...

The Tip of the Iceberg

- Employee cyber-privacy claims certainly present a new realm of considerations for insurers, regardless of the medium.
- However, employers can run into problems when an employee improperly uses data just as easily as when the employer does.
- These “data breach” claims represent much more complicated, and costly, claims than the majority of EPL-related matters.

Data Breach Claims

Data Breach Claims

- While Employment Practices claims present a distinct challenge to Insured employers - and therefore Insurers - the loss, compromise, or misuse of electronic data presents a more nuanced, and potentially more severe, risk.

Data Breach Claims

- A data breach can cost millions of dollars, based on the type and amount of data effected.
- Any entity that stores third-party data can be at risk, including (but certainly not limited to):
 - Retailers
 - Financial institutions
 - Health care providers

Data Breach Claims

- The potential claims are at least as varied as the potential claimants:
 - Actual loss (theft) of customer, client or employee data
 - Extortion based on a threatened loss of customer, client or employee data
 - Monitoring or repairing of credit reports for those effected by a data breach
 - Notices issued to those effected by a data breach
 - Public relations activity necessitated by a data breach
 - Remediation and repair of systems due to a data breach
 - Lost profits caused by a data breach

Data Breach – Important Questions

- Once a data breach occurs, several important questions must be addressed:
 - What type of data was involved?
 - What was the cause of the breach?
 - What are the sources of potential loss to the Insured?
 - What are the potential damages to which the Insured is exposed?
 - What needs to be done to mitigate the breach?

Data Breach – Data Involved

- What type of data was involved?
 - Personally Identifiable Information (PII) is the most common, and will be the focus here:
 - First name or initial combined with a social security number, driver’s license number, state ID number, or account number with access code or password
 - Other sources of potential concern include proprietary data of a vendor or internal proprietary data.

Data Breach – Cause of the Breach

- What was the cause of the breach?
 - The cause of the breach can effect both potential liability and coverage:
 - External hacking
 - Wrongdoing internal to the insured
 - Failure of controls or preventative measures
 - Failure of hardware or software
 - Wrongdoing or failure of a vendor or other related third-party entity

Data Breach – Sources of Loss

- What are the sources of potential loss to the insured?
 - While the most common (and most elusive) source of loss is a civil action by the individual effected by the breach, there are other sources of potential liability for the insured:
 - Violation of "Red Flag Rules" (requiring entities to implement an identity theft prevention program) under the Fair and Accurate Credit Transactions Act, enforced by the Federal Trade Commission ("FTC")
 - Health Information Technology for Economic and Clinical Health Act, enforced by the FTC and the Department of Health and Human Services
 - Children's Online Privacy Protection Act
 - CAN-SPAM Act
 - Gramm-Leach-Bliley Act
 - Fair Credit Reporting Act
 - Computer Fraud and Abuse Act
 - Federal Privacy Act
 - State attorney general actions and consumer protection laws

Data Breach – Potential Damages

- What are the potential damages to which the insured could be exposed?
 - Depending on governmental involvement, the strategy of the claimant, and the approach of the Insured, multiple damages are possible:
 - Compensatory damages (although difficult to prove)
 - Consequential damages
 - Punitive damages
 - Fines and fees (imposed by regulatory agencies)
 - Remediation of hardware and software
 - Lost profits and goodwill
 - Notification of effected individuals/entities
 - Monitoring of effected individuals/entities

Focus on Cyber-Liability Laws - *Federal "Red Flags" Rules*

- In addition to civil liability for the actual loss of customer data, Insureds can now face regulatory penalties for allowing a data breach.
- The "Red Flags Rules," were promulgated under the Fair and Accurate Credit Transactions Report Act. 16 CFR 681.1.
- Require certain entities to identify relevant Red Flags, detect their occurrence, and respond appropriately to protect customer data.
- "Red Flag" is defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft."
- An Insured without proper procedures in place can face liability not only for the loss of data, but also for the failure to prevent it.

Focus on Cyber-Liability Laws - *Evolution of the Common Law*

- Cyber-liability concerns have also caused an evolution in the common law.
- For example, conversion claims may now apply equally to electronic data, as opposed to traditional notions of tangible goods.
- Accordingly, an employer may be liable for the value of an employee's electronic data the employer appropriates, even if stored on the employer's hardware. See *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E. 2d 1272 (N.Y. 2007).
- An Insured must be wary of an expansion of all sources of liability when dealing with employee data.

**Data Breach –
Risk Mitigation**

- What needs to be done to mitigate the effect of a data breach?
 - Once a breach has occurred, the insured has multiple options for mitigating the breach (some of which may impact coverage).
 - Incident analysis (internal communication, containment, harm determination)
 - Incident disclosure (notice to effected individuals, vendors, regulatory agencies)
 - Loss mitigation (trending, benchmarking, remediation)

Data Breach - The Bottom Line

- When a data breach occurs, immediate and decisive action is required:
 - Evaluate the potential scope of the loss, in terms of individuals effected
 - Identify the governmental and regulatory agencies with whom communication is necessary
 - Understand how mitigation strategies effect costs and coverage

Data Breach - The Bottom Line

- The plan of action will vary from claim to claim:
 - In some situations—for example where the compromised data is very sensitive or the breach malicious—a proactive or aggressive measure (such as credit monitoring for effected individuals) may be required to protect said individuals and reduce long-term costs.
 - In situations where large amounts of data are borderline PII, a more reactive approach may be more cost-effective and responsible.
- In every situation, the claims adjuster and retained counsel must ensure proper handling of a data breach, and guide it through the most effective resolution.

Insurance For Cyber Claims

Gaps in Traditional Insurance Policies

- Property Insurance policies – “Property” is usually defined to be “tangible” property and does not cover loss of “intangible” property like data.
- Crime/Fidelity policies – Generally do not cover theft of confidential or proprietary information, as they are not “tangible” property.
- General Liability policies – Most GL Policies include exclusions for damages arising from internet and technology activities. Additionally, GL policies do not typically cover losses associated with unauthorized access by third parties.
- Errors & Omissions policies – Generally exclude security breaches or damages arising from unauthorized access.
- EPL policies – Not covered by Insuring Clauses.

Cyber-Privacy vs. Data Breach Claims

- While employee cyber-privacy claims represent a new avenue for an insured’s liability, existing EPL policies traditionally apply to such claims.
- More problematic are the claims arising from an insured’s data breach claim, due to its unique sources of loss.
 - As a result, many insurers have responded by issuing policies and endorsements that address cyber-related liability, in all its forms.

Cyber Liability – Covered Risks

Generally, cyber liability policies address two types of risks:

- First Party: losses suffered directly by the Insured
- Third Party: losses associated with the Insured's liability for damages suffered by a third party

First Party Losses

First party losses in the context of a cyber liability loss would include:

- Business interruption costs
- Crisis management and public relations costs
- Privacy notifications and credit monitoring costs
- Costs associated with theft or vandalism of a company's network or systems
- Upgrades in network security

Third Party Losses

Third party losses in the context of a cyber liability loss would include:

- Disclosure Injuries: unauthorized access to or dissemination of a third party's private information
- Content Injuries: copyright, trademark, trade secrets or other intellectual property claims
- Reputation Injuries: libel, slander, defamation, invasion of privacy claims
- System Injuries: security failures or virus transmissions that harm the computer systems of third parties
- Impaired Access Injuries: customers cannot access their accounts or information

**Methods of Addressing
Cyber Risks**

- Stand alone Cyber Liability Policies
 - First Party Loss Policies
 - Third Party Liability Policies
 - First Party/Third Party Combined Policies
- Cyber specific Endorsements added to Traditional Policies

**First Party Losses in
Third Party Claims**

- Often a third party liability claim will involve direct losses by the Insured
 - A third party cyber liability policy may provide coverage for certain direct losses associated with a claim (or a potential claim) by a third party. These may include:
 - Security breach notifications
 - Credit monitoring costs
 - Crisis management consultation

Cyber Liability Coverage by Endorsement

- Insurers have customized traditional Policies to provide additional coverage for specific cyber risks by endorsements.
For example:
 - EPLI Policies – coverage for employee related theft or third party unauthorized access to private information.
 - E&O Policies – coverage for e-commerce activities, security breaches, and unauthorized access
 - Property & Crime Policies – coverage for “intangible” property like data
