CYBER LIABILITY PRIMER

Steven D. Strang, Esq.
sstrang@gallaghersharp.com
Rema A. Ina, Esq.
rina@gallaghersharp.com

I. PRIVACY LAWS

A. History of Privacy

"Privacy" is not mentioned in the U.S. Constitution. The concept is first addressed in Supreme Court case law in *Olmstead v. United States*, 277 U.S. 438 (1928), where Justice Brandeis articulated a general constitutional right "to be left alone," which he described as the most comprehensive and valued right of civilized people.

The right of privacy protected by the Constitution gained a foothold in *Griswold v. Connecticut*, 381 U.S. 479 (1965), where the Supreme Court struck down a state statute forbidding married adults from using birth control because the statute violated the sanctity of the marital bedroom. The Court held that a general right to privacy may be inferred from the express language of the First, Third, Fourth, Fifth, and Fourteenth Amendments.

B. Present Day Privacy Laws

The United States has no omnibus privacy law. Europe does.

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. The GDPR was approved and adopted by the EU Parliament in April 2016 and came into force on May 25, 2018. See https://eugdpr.org/the-regulation

The California Consumer Privacy Act (CCPA), which was signed into law in June 2018 by Governor Jerry Brown, is the first United States law following in the footsteps of GDPR. See https://oag.ca.gov/privacy/ccpa.

1. **Federal Level:** In the United States privacy laws are enforced at the Federal and State level by a variety of organizations.

a. ***FTC:*** In the US privacy issues are often treated as consumer issues, so the FTC is the agency with the bulk of privacy-related responsibilities. (IAPP: Principles of Privacy in the US Private Sector). The FTC brings complaints against organizations employing deceptive or unfair practices:

(1) "Unfair" – The injury must be substantial, it must be without offsetting benefits, and it must be one that consumers cannot reasonably avoid.

(2) FTC has taken action against Gateway, Google, BJ's, and Facebook. Gateway promised not to sell consumer information, and it did. (IAPP: Principles of Privacy in the US Private Sector).

(3) The FTC can impose civil penalties, or enter into a consent decree such as subjecting a company to privacy audits by third-parties.

b. ***HIPAA*****:** Health Insurance Portability and Accountability Act of 1996. HIPAA, passed in 1996, protects the disclosure of protected health information, defined as "any individually identifiable information." (IAPP: Principles of Privacy in the US Private Sector)

(1) Extremely comprehensive.

(2) HITECH, passed in 2009, enhanced patient's privacy rights and provided new rights to a patient's right to copies of health care information. The 2013 amendment to HIPAA incorporated the requirements of HITECH. This increased the potential for a HIPAA violation following a disclosure of personal health information. Laura E. Bange and Amy S. Locke, Esq. RPLU, "Insurability of HIPAA Claims Arising From Health Information Data Breaches Under Traditional E&O and D&O," *Prof. Liab. Underwriting Society Journal*, Vol. XXVII, No. 7, July 2014.

(3) The Secretary of the U.S. Department of Health and Human Services must be notified contemporaneously with the individual of any breach on unsecured PHI that involves 500 or more individuals. From September 23, 2009 to December 31, 2012, there were 710 reports of such data breaches affecting a total of approximately 22.5 million individuals. U.S. DEPT. OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, Annual Report to

Congress on Breaches of Unsecured Protected Health Information (2011-2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html.

(4) Applies only to "health care providers" or those who perform services for health care providers.

(i) Applies to health insurers, but not home owners insurers or automobile insurers

(5) Does not apply to lawyers, BUT provides a reference point for what sort of information should be kept private.

c. ***USA Patriot Act.***

d. ***Video Privacy Protection Act.***

e. ***Telemarketing and Consumer Fraud and Abuse Prevention Act.***

f. ***Family Educational Rights and Privacy Act of 1974 (FERPA)***: Addresses student records.

(1) Why you cannot get your college student's grades unless the student signs a waiver.

(2) No private right of action (IAPP: Principles of Privacy in the US Private Sector)

g. ***Fair Debt Collection Practices Act:*** Passed in 1977 and prohibits debt collectors from using abusive, unfair, or deceptive practices in the collection of consumer debt. It also protects against the disclosure of a consumer's private and confidential account information by debt collectors.

h. ***Gramm-Leach-Bliley Act:*** Passed in 1999, governs financial institutions that collect nonpublic personal information, and is used primarily for personal, family, or household purposes. The Act requires such institutions to provide privacy notices, restricts disclosure of nonpublic personal information to third parties, and allows consumers to opt out to prevent their information from being shared.

i. ***Children's Online privacy Protection Act (COPPA):*** Applies to commercial website that are directed to children under 13. The most enforced privacy regulation in the US and has the stiffest

penalties. Enforced by the FTC. (IAPP: Principles of Privacy in the US Private Sector).

j. ***The Fair and Accurate Credit Transactions Act (FACTA):*** Passed in 2003, reduces the risk of identity theft by regulating the handling of consumer account information and applies to any type of organization that collects credit information.

2. **State Level:** At the state level privacy violations are generally enforced by the Attorney General.

a. ***Ohio's Breach Notification Law:*** Ohio Revised Code §1349.19 requires notification to Ohio residents if there is a security breach which puts their personal information at risk for identity theft or fraud.

(1) "Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state." R. C. § 1349.19(B)(1).

(2) "Breach of the Security System" means: "unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state." R.C. § 1349.19(A)(1)(a).

(3) Ohio's notification law applies to businesses, such as law firms or individuals that conduct business in Ohio and own or license computerized data. The data must include personal identification data information of an Ohio recipient. *See Losch & Assocs., Inc. v. Polonczyk*, 2016 WL 3856112 at *3 (Ohio Ct. App. 1st Dist. July 15, 2016).

(4) The disclosure must be made in the most expedient time possible, but no later than 45 days after the discovery of the breach. R. C. § 1349.19(B)(2).

(5) Failure of compliance with Ohio's reporting statute can result in the Attorney General conducting an investigation and bringing a civil action.

(6) Content: Ohio does not specify what the communication must include. However, North Carolina requires things such as:

(i) A description of the incident.
(ii) The information breached.
(iii) What the business has done to prevent further loss.
(iv) Who to call for assistance.
(v) A warning to remain vigilant (N.C. Gen. Stat. §§75-65).

(7) Exceptions: Some states have an exception to disclosure if the data is encrypted.

R.C. 1349.19(A)(7)(a) states that "'Personal information' means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, *when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable*." (Emphasis added.)

b. ***Ohio's Privacy Act*:** Ohio Revised Code 1347.10(A)(2), makes a person liable for wrongful disclosures of personal information.

(1) R.C. 1347.01 defines "personal information" to mean "any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a

name, identifying number, symbol, or other identifier assigned to a person."

(2) R.C. 1347.01 is broad, and would include:

(i) Names.
(ii) Social security numbers.
(iii) Addresses and phone numbers.
(iv) Driver's license numbers and/or state identification numbers.
(v) Financial account information and tax information.
(vi) Health records, physical characteristics or other biometrics.
(vii) Education information.

Statute states as follows: "A person who is harmed by the use of personal information that relates to him and that is maintained in a personal information system may recover damages in a civil action from any person who directly and proximately caused the harm by doing any of the following:

> (2) Intentionally using or disclosing the personal information in a manner prohibited by law * * *." (Emphasis added.)

Generally, personnel records relating to public employees are public records unless an exception applies. Items contained in background investigation files regarding police candidates, including investigatory reports compiled by law enforcement agencies to assist in employment decisions, generally are not confidential law enforcement records. *Patrolman X v. Toledo*, 132 Ohio App. 3d 374 (Ohio C.P. 1996)

c. ***Ohio Data Protection Act:*** Went into effect on Nov. 2, 2018. Offers company a defense if it suffers a data breach:

(1) The DPA provides "covered entities"-- essentially any business that "accesses, maintains, processes, or communicates" personal or restricted information -- a legal safe harbor in the event they do get breached, but only if they follow and maintain a cybersecurity framework in accordance with reasonable or recognized industry standards. To encourage compliance, the DPA explicitly avoids setting minimum data security levels or imposing

liability on businesses that fail to maintain cybersecurity programs in compliance with the law.

(2) To qualify for safe harbor, a business must "create, maintain, and comply with a written cybersecurity program" that "reasonably conforms" to one of several industry-recognized cybersecurity frameworks, including:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- NIST Special Publications 800-53, 800-53A, or 800-171.
- Federal Risk and Authorization Management Program (FEDRAMP).
- Center for Internet Security Critical Security Controls (CIS CSC).
- International Organization for Standardization (ISO) / International Electrotechnical Commission's (IEC) 27000 Family.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule Subpart C.
- Health Information Technology for Economic and Clinical Health Act (HITECH).
- Title 5 of the Gramm-Leach-Bliley Act of 1999 (GLBA).
- Federal Information Security Modernization Act of 2014 (FISMA).
- Payment Card Industry standard (PCI) plus another listed framework.

(3) To qualify, the business must implement a cybersecurity program designed to: (1) protect the security and confidentiality of personal information; (2) protect against any anticipated threats or hazards to the security or integrity of personal information; and (3) protect against unauthorized access to and acquisition of personal information.

(4) The DPA notes that measures taken depend on the size, type of information, and industry of the business. Under the DPA, an effective program must be scaled to match:

a. The size, complexity and nature of the business and its activities;
b. The sensitivity level of personal information the business possess;

c. The cost and availability of tools to improve the security and reduce vulnerabilities; and
d. The resources the business has at its disposal to expend on cybersecurity.

(5) Businesses must be aware that the DPA does not create blanket immunity, but merely creates an affirmative defense to tort actions brought against compliant businesses that suffer data breaches. The business maintains the burden of establishing that its cybersecurity program is compliant with the DPA. The DPA only applies to Ohio tort claims (not contractual disputes).

(6) DPA does not alter the current breach notification laws.

d. ***Legal Requirements for "Reasonable Security."*** Security is relative but a new legal standard for reasonable security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach that involves a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments. (Jill D. Roadies and Robert S. Litt, *The ABA Cybersecurity Handbook*, 2nd Edition, p. 73.)

3. **What is private information?** Certainly social security numbers, but what about buying habits?

Example:

New parents are the "holy grail" of retailers because they are buying a lot of new items, and will likely continue to do so for the foreseeable future. It is one time in a person's life where their spending habits will change. Therefore it is very important for stores to get to them. Since birth records are public information, many companies send promotional materials when the child is born.

Target wanted to beat the rush. The company has collected vast amounts of data on every person who regularly walks into one of its stores. Whenever possible, Target assigns each shopper a unique code — known internally as the Guest ID number — that keeps tabs on everything they buy. So, they ran data and identified 25 products that women tend to buy when pregnant. For example: women buy more unscented lotion at the beginning of the second trimester, and generally buy more supplements,

cotton balls, hand sanitizers, and washcloths. Target could then assign them a "pregnancy score."

About a year later a man walked into a store with pregnancy coupons sent to his high school daughter, irate that the store was encouraging his daughter to get pregnant. The man called Target back few days later and apologized –his daughter confessed to being pregnant.

After the story was published in the *New York Times* there was a tremendous backlash, and Target apologized. They no longer make their targeted marketing as obvious.

http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&hp=&pagewanted=all

II. CYBER RISKS

According to an October 3, 2018 Cyber Liability Seminar held by the FBI, the FBI field office in Cleveland receives 3-4 calls about business email compromises every week. These are for the most part not large companies.

A. Tort Exposure.

1. General negligence theory:

   a. It could be argued that there is a "duty" to keep someone's personal information protected if you are entrusted with it, particularly in a business context.

   b. Of course: "A client's claims that arise out of the manner in which an attorney represents the client within the attorney-client relationship, regardless of the names affixed to the theories of recovery or causes of action, are claims for legal malpractice." *Sprouse v. Eisenman*, 2005-Ohio-463, ¶8 (10th Dist.). Such claims, "regardless of their phrasing or framing, constitute legal malpractice claims…." *Sandor v. Marks*, 2014-Ohio-685, ¶10 (9th Dist.).

2. Professional negligence theory; this is particularly relevant to lawyers.

3. Invasion of privacy theory:

   a. In the syllabus in *Housh v. Peth*, 165 Ohio St. 35 (1956), the Supreme Court of Ohio stated:

(i) The right of privacy is the right of a person to be left alone, to be free from unwarranted publicity, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.

(ii) An actionable invasion of the right of privacy is the unwarranted appropriation or exploitation of one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities.

b. In Ohio, the tort of invasion of privacy includes four distinct causes of action: (1) intrusion into plaintiff's seclusion, solitude, or private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity that places plaintiff in a false light; and (4) appropriation of plaintiff's name or likeness for defendant's advantage. *Yoder v. Ingersoll-Rand Co.*, 1998 U.S. App. LEXIS 31993 (6th Cir. Ohio Dec. 22, 1998)

c. The public disclosure variety of the tort of invasion of privacy has at least three requirements: (1) a clearly private fact; (2) public disclosure of the private fact; and (3) a showing that the matter made public is one which would be highly offensive and objectionable to a reasonable person. *Id.*

d. In *Yoder*, the plaintiff's status as an AIDS patient was disclosed accidentally by his employer to his mother, who worked at the same company. The Sixth Circuit affirmed summary judgment, finding that while the plaintiff met the first and third prongs, finding that "Publicity," as used in the second prong, means "communicating the matter to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." Disclosure to a *single person* is not sufficient. *Id.* at *6-7.

(i) The court also found that the Supreme Court of Ohio would likely not require the disclosure to be intentional.

(ii) Leaves open the question of whether a data breach would be actionable.

e. Courts have found intrusion into seclusion claims to be analogous to "an intentional tort analogous to trespass and battery in protection of personal integrity… A mere negligent intrusion into

one's private activities does not constitute an actionable invasion of the right of privacy. " *McCormick v. Haley*, 307 N.E.2d 34 (10th Dist. 1973). *See, also, Yoder*.

(i) Many of these cases stem from the purposeful transmission of junk faxes or telephone solicitation.

B. Damage to Reputation.

1. Company reputation.

2. Individual employees' reputation.

3. Third parties' reputation.

C. Business Interruption Losses and Loss of Income.

1. Loss of earnings and expenses incurred due to an interruption in the system. This coverage typically involves a waiting period, or time that has to elapse before the issues is covered, which is typically eight hours.

2, The average cost of a data breach increased 6.4 percent in 2018 to $3.8 million, according to IBM. (Donna Rice, "Data Breaches and Record Retrieval: Protect Your Firm in 2019," *CLM Magazine*, March 2019).

3. The global cost of cyber crime is predicted to hit $6 trillion annually by 2021. Press Release, Cybersecurity Ventures, "Cybersecurity Economic Predictions: 2017 to 2021," (Oct. 19, 2016).

E. Risks For Lawyers

1. Lawyers routinely handle personal information. Litigators may correspond with opposing counsel about a client's personal health information; send discovery responses over email that contain the client's address, medical records, and social security number; and file records with a court such as deposition transcripts which contain a client's address, phone number, social security number, occupation, and date of birth. Estate planning attorneys may exchange sensitive tax information and documents over email. Transactional attorneys may exchange corporate information over email, and save sensitive corporate information on their internal systems which likely have fewer safeguards than their client companies.

2. Ohio has identified by statute certain types of protected personally identifiable information - R. C. 1347.01:

(1) Names

(2) Social security numbers and records
(3) Résumés
(4) Correspondence
(5) Addresses and phone numbers
(6) Driver's license numbers and/or state identification numbers
(7) Professional license numbers
(8) Financial account information and tax information
(9) Health records, physical characteristics or other biometrics
See, also, Health Insurance Portability and Accountability Act of 1996 (HIPAA)
(10) Education information
(11) Salary and job classifications
(12) Performance evaluations, employment applications, timesheets

3. Why Lawyers?

a. *Law Firms are attractive targets for hackers*: Law firms possess the same valuable data of their clients without the increased security. Further, attorneys habitually transmit confidential information about their clients, or other third parties offsite. Simply put, law firms are easy targets for hackers.

b. *Increased susceptibility*: The FBI has noted the increased susceptibility of law firms for cyber breaches. The Bureau met with 200 of New York City's leading firms to address the rising number of cyber breaches and to warn attorneys they are the "back door" to their corporate clients. Michael A. Riley and Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data," Bloomberg (Jan. 31, 2012) *available at* https://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms.

c. A recent study of cybersecurity practices at over 200 law firms found that each one had been targeted for confidential data, and over 40 percent did not know they had been breached. LogicForce, Law Firm Cyber Security Scorecard, Q1, 2017, *available at* https://www.logicforce.com/2018/03/28/law-firm-cyber-security-scorecard.

d. "This case [*United States v. Iat Hong*] of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals." Preset Bharara,

United States Attorney, Southern District of New York, Press Release 2016.

e. A security breach of a law firm could have serious consequences for clients and even innocent third parties. It could subject them to identify theft, fraud, negative publicity, and even financial ruin. If a law firm loses client information, the reputational harm alone may lead to loss in business or even involve an ethical violation. (Jill D. Roadies and Robert S. Litt, *The ABA Cybersecurity Handbook*, 2nd Edition, p. 16.)

4. Types of Breaches

According to Willis Towers Watson, the following are the percentage of claims by breach type:

a. Accidental disclosure – 32.72% – this includes sending email to the wrong party.

b. Lost/stolen devices – 21.43% – losing your smartphone, laptop, hard drive, or other portable media containing encrypted personal information, including medical, education, and financial records.

In March 2017, Horizon Healthcare Services, Inc. agreed to pay $1.1 million and improve its security practices after two laptops containing the personal information of 690,000 New Jersey policyholders were stolen. The data was not encrypted as required by federal law. (Mark Iandolo, "Horizon Healthcare Services Settles Data Breach Case for $1.1 Million," *Legal Newsline* (Mar. 1, 2017) *available at* https://legalnewsline.com/stories/511085361-horizon-healthcare-services-settles-data-breach-case-for-1-1-million.

c. Hack – 17.28%

Access through unsecured wireless networks: Public WiFi locations generally do not have security features necessary to protect confidential data. Hackers often use fake Wi-Fi hotspots to intercept or re-direct confidential information.

Unsecured cloud service: Storing documents in a cloud service such as Dropbox creates risks. The cloud should be considered a public repository, and sensitive documents should be encrypted before they are placed there.

California Bar Formal Opinion No. 2010-179:

(1) Facts: A law firm provided an attorney a laptop computer for his use on client and firm matters. The attorney used the laptop at a local coffee shop and accessed a public wireless Internet connection to conduct legal research on a matter and e-mailed a client. He also used the laptop at home on his personal wireless system to conduct research and e-mail a client.

(2) Based upon California's Professional Conduct and Evidence Rules, the attorney risked violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on a client's case because of the lack of security features on many public wireless locations. The attorney would not violate his duties if he took the appropriate precautions, such as using a personal firewall, file encryption, and encryption of wireless transmissions.

d. Rogue employee – 11.52%

e. Business interruption – 2%

Weiss, Brian, "The Human Element of Cyber Risk," *Cyber Claims Brief*, Willis Towers Watson, 2016

6. Who has standing to sue?

In *Frank v. Gaos,* The United States Supreme Court may finally weigh in on whether a demonstration of actual harm is required for standing to sue in data breach litigation. The circuit courts are currently split. The 3rd, 6th, 7th, 11th and D.C. circuits have generally found standing if the plaintiffs can demonstrate a heightened "risk of future harm." The 1st, 2nd, 4th, 5th, and 9th circuits have found no standing to sue absent actual harm. (Joseph J. Lazzarotti and Maya Atrakchi, "Workplace Privacy, Data Management & Security Report," Jackson Lewis, February 12, 2019).

III. BEST PRACTICES AND THINGS TO CONSIDER

Ten IT Security Best Practices (In No Particular Order)

1. *Encrypt Data:* Encryption of data (at rest and in transit) is essential to protecting sensitive data and to help prevent data loss due to theft or equipment loss. Implement whole disk encryption on all mobile devices.

2. *Use Digital Certificates:* Obtain SSL certificates from one of the trusted authorities. Install certificates on hardware devices such as routers, servers or load balancers.

3. *Implement DLP and Auditing:* Use data loss prevention and file auditing to monitor, alert, identify, and block the flow of sensitive customer data (e.g. Social Security Numbers, Personal Health Information (PHI), account numbers … etc.) into and out of the network.

4. *Implement a Removable Media Policy:* Restrict the use of USB drives, external hard disks, thumb drives, external DVD writers, and any writeable media. These devices facilitate security breaches coming into or leaving the network.

5. *Scan for Attack Surfaces and Vulnerabilities:* Perform regular and periodic remote and internal Penetration Tests and Vulnerability Scans (Nessus, Qualys, Rapid 7, Metasploit, SecureWorks) against company servers Scan internally-hosted company website(s) daily for malware, set the Secure flag for all session cookies, use SSL certificates with Extended Validation.

6. *Implement an Email Spam/Content Filter:* Use a spam filter to remove unwanted or suspicious email from entering user inboxes and junk folders. Teach users how to identify junk mail even if it's from a trusted source.

7. *Implement a Comprehensive Endpoint Security Solution:* Use a multi-layered product to prevent and/or remediate malware infections on user devices (desktops, laptops, tablets, smartphones … etc.). Keep in mind that antivirus software alone is not enough. Antivirus, personal firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) and Mobile Device Management (MDM) are all part of the total approach to endpoint protection.

8. *Implement Network-based Security Hardware and Software:* Use enterprise firewalls, antivirus, intrusion detection devices, honey pots, and monitoring to screen for DoS attacks, virus signatures, unauthorized intrusion and ex-filtration, port scans, and other network attacks and attempts at security breaches.

9. *Maintain Security Patches:* Update antivirus programs on a daily basis. Be sure that your software and hardware defenses stay up to date with new antimalware signatures and the latest patches. If you turn off automatic updating, set up a regular scan and remediate plan for your systems.

10. *Educate Users:* User awareness might be the most important non-hardware, non-software solution available. An informed user is a user who behaves more responsibly and takes fewer risks with valuable company data, including email.

IV. COMMON POLICIES FOR LAWYERS FOR CYBER CLAIMS

A. Professional Liability Policy

1. *Covers professional services.* They are generally claims-made, meaning that the policy in place when a "claim" is brought against the lawyer applies rather than the policy in place at the time of the alleged negligent act or omission.

   Example: You have a client injured in a motor vehicle accident on July 4, 2014. You miss the July 4, 2016 statute of limitations period. The client sues you on May 4, 2017. The policy in place on May 4, 2017 applies.

2. *Claims-made v. claims-made and reported.*

   It is important to note the difference. *U.S. v. A.C. Strip*, 868 F.2d 181, 187 (6th Cir 1989). If your policy is claims-made, the policy in place at the time the claim is made against you applies, and generally you have to report the claim to your insurer within a reasonable time period, even if you report the claim *after* the policy expires. If your policy is claims-made and reported, the claim has to be made against you and you have to turn around and report it to the insured within the policy period as well. Case law shows this provision is enforced. *U.S. v. A.C. Strip*, 868 F.2d 181, 187 (6th Cir 1989).

B. Commercial General Liability Policy

1. Applies to bodily injury or loss of tangible property caused by "an occurrence."

2. General liability policies have an exclusion for cyber-perils, and specifically exclude "electronic data" from the definition of "property damage." Insurers are clarifying that cyber perils are not covered. Several insurers have revised the definition of "property damage" in CGL policies to include:

   > "For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment." (Siwik, Lori L., Warmbir, Jason, Regal, Dorothea W., Wong, Ray, Kasper, Kathryn, "Risky Business with Cyber Insurance—

Sunglasses Not Optional," Insurance Coverage Litigation Committee, American Bar Association, March 2-4, 2017)

3. Case law suggests that computer data is not "tangible property" because it lacks a physical substance.

   a. *Ward v. Gen. Servs. Inc. v. Employers Fire Ins. Co.,* 114 Cal App. 4th 548, 556-57 (where a computer crash due to human error resulted in data loss, the court held that there was no physical loss or damage. The data loss was simply a "loss of organized information" and concluded that the information cannot be said to have a material existence, be formed of tangible matter, or be perceptible to the sense of touch).

   b. *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 93-98 (4th Cir. 2003) (finding that "physical magnetic material on the hard drive is tangible" but software and data are not).

C. Crime Policy

1. Policy will have multiple grants of coverage, and a policyholder can select which to include when purchasing coverage. The different types include:

   a. *Fidelity* – Employee theft or employee dishonesty, insures against employee theft.

   b. *Forgery or alteration* – May provide defense cost coverage if the insured is sued on a note based upon the claim that it was forged or altered.

   c. *On premise*s – Insures against loss of money or securities located on the insured's premises, including by theft. Also covers damage to property like a safe.

   d. *Money orders and counterfeit money*.

2. These policies apply to more traditional avenues of theft, and do not cover negligent breaches or liability to third-parties.

D. Cyber Policies –Requirements for Lawyers

1. *Gov. Bar R. III, Section 4. Financial Responsibility:*

   (A) A legal professional association, corporation, legal clinic, limited liability company, or limited liability partnership shall maintain adequate professional liability insurance or other form of adequate

financial responsibility for any liability of the firm arising from acts or omissions in the rendering of legal services by an officer, director, agent, employee, manager, member, partner, or equity holder.

(1) "Adequate professional liability insurance" means one or more policies of attorneys' professional liability insurance that insure the legal professional association, corporation, legal clinic, limited liability company, or limited liability partnership both:

(a) In an amount for each claim, in excess of any deductible, of at least fifty thousand dollars multiplied by the number of attorneys practicing with the firm; and

(b) An amount of one hundred thousand dollars for all claims during the policy year, multiplied by the number of attorneys practicing with the firm. No firm shall be required to carry insurance of more than five million dollars per claim, in excess of any deductible, or more than ten million dollars for all claims during the policy year, in excess of any deductible.

(2) "Other form of adequate financial responsibility" means funds, in an amount not less than the amount of professional liability insurance applicable to a firm under Section 4(A)(1) of this rule for all claims during the policy year, available to satisfy any liability of the firm arising from acts or omissions in the rendering of legal services by an officer, director, agent, employee, manager, member, partner, or equity holder. The funds shall be available in the form of a deposit in trust of cash, bank certificate of deposit, or United States Treasury obligation, a bank letter of credit, or a surety bond.

(B) Each member, partner, or other equity holder of a legal professional association, corporation, legal clinic, limited liability company, or limited liability partnership shall be jointly and severally liable for any liability of the firm based upon a claim arising from acts or omissions in the rendering of legal services while he or she was a member, partner, or equity holder, in an amount not to exceed the aggregate of both of the following:

(1) The per claim amount of professional liability insurance applicable to the firm under this rule, but only to the extent that the firm fails to have the professional liability insurance or other form of adequate financial responsibility required by this rule;

(2) The deductible amount of the professional liability insurance applicable to the claim. The joint and several liability of the member, partner, or other equity holder shall be reduced to the extent that the liability of the firm has been satisfied by the assets of the firm.

(C) Each officer, director, agent, employee, manager, member, partner or equity holder of a legal professional association, corporation, legal clinic, limited liability company, or limited liability partnership shall be liable for his or her own acts or omissions as provided by law, without prejudice to any contractual or other right that the person may be entitled to assert against a firm, an insurance carrier, or other third party

2. *Ohio Rule of Prof. Cond. 1.4:*

Rule 1.4(c) of the Rules of Professional Conduct requires an attorney to advise a client in writing with the client's signed acknowledgment, if the attorney does not maintain professional liability insurance in the amount of at least $100,000 per occurrence and $300,000 in the aggregate or if the lawyer's professional liability insurance is terminated.

Comment [8] provides: "Although it is in the best interest of the lawyer and the client that the lawyer maintain professional liability insurance or another form of adequate financial responsibility, it is not required in any circumstance other than when the lawyer practices as part of a legal professional association, corporation, legal clinic, limited liability company or limited liability partnership."

Cyber liability insurance has been available for more than a decade, but is not specifically required by the Rules of Professional Conduct, which require only "professional liability insurance."

3. *In August, 2014, the American Bar Association adopted Resolution 109 encouraging cyber security plans:*

"RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cyber security program that complies with applicable ethical

and legal obligations, and is tailored to the nature and scope of the organization, and the data systems to be protected."

4. *Ohio Rules of Professional Conduct require an attorney to act competently.*

1.1 COMPETENCE

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

Comment [8] Maintaining Competence:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

5. *Ohio Rules of Professional Conduct require an attorney to maintain the confidentiality of a client's information.*

1.6: CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not reveal information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law, unless the client gives *informed* consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by division (b) or required by division (c) of this rule.

(b) A lawyer shall make *reasonable* efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information related to the representation of a client.

Comments [18-19] Acting Competently to Preserve Confidentiality[1]

[1][18]: ***Division (c) requires*** a lawyer to act competently to safeguard information relating to the representation of a client against ***unauthorized access by third parties*** and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The unauthorized access to or the inadvertent or unauthorized disclosure of information related to the representation of a client does not constitute a violation of division (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the 35 safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A

V. CYBER POLICY PROVISIONS

A. What does a cyber policy cover?

1. They can provide "first-party" coverage for crimes against the policyholder, as well as "third-party" coverage relative to claims against the policyholder. They are generally claims-made.

2. First-party damages are typically defined as damages suffered by the policyholder to their own property and include replacement costs and remediation.

   Cyber Insurance is generally offered as a stand-alone product although the marketplace is evolving allowing smaller businesses to acquire cyber insurance as part of a package. (Jill D. Roadies and Robert S. Litt, *The ABA Cybersecurity Handbook*, 2nd Edition, p. 320.)

3. Cyber policies can include:

   a. Data loss, such as that resulting from a stolen laptop
   b. Privacy breaches from an employee losing a smartphone with client information, such as use of that information to sign up for a credit card
   c. Regulatory actions like fines and penalties
   d. Payment Card Industry (PCI) assessment claims
   e. Business income or interruption losses. Example: An online retailer is hacked on Black Friday, causing its website to crash and an inability to take orders.
   f. Losses from the firm's IT vendors
   g. Notification of affected customers if there was a data breach

---

client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forego security measures that would otherwise be required by this rule. ***Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state or federal laws that govern data privacy or that impose specific notification requirements upon the loss of or unauthorized access to electronic information is beyond the scope of these rules***….

[19]: When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws governing data privacy, is beyond the scope of these rules.

h. Forensic services to determine whether a breach has occurred
i. Cyber extortion coverage

4. Cyber policies often will provide coverage with costs associated with a potential privacy breach even if there is never a liability claim, and can include crisis management costs.

5. Cyber policies are not written on "standard forms," meaning each insurer has traditionally written its own unique policy with unique policy language. (Aldama, Karin S., Eyerly, Tred R., "Cyber Policies–The Next Wave," Coverage Litigation Committee, American Bar Association, March 1, 2018).

6. Analyzing coverage is difficult because there is still little case law interpreting the language. (Aldama, Karin S., Eyerly, Tred R., "Cyber Policies–The Next Wave," Coverage Litigation Committee, American Bar Association, March 1, 2018). Most case law interprets non-cyber policies such as CGL policies as to cyber claims.

7. Cyber policies do not include everything related to computers, though. In *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co.*, No. CV-15-01322, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. 2016), the court held that the cyber liability policy did not provide coverage for over $1.9 million in fees and assessments that P.F. Chang's was required to pay Bank of America, which provided credit card processing services. Hackers stole the credit card information of over 60,000 P.F. Chang's customers, and Bank of America had to reimburse over $1.9 million to Mastercard as a result of the contract between the companies. It then filed suit against P.F. Chang's to recoup the money, which tendered the claim to its insurer.

   Federal's cyber policy provided coverage for claims made against the insured for covered injury, including a "Privacy Injury," defined as an "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record…." The policy also contained an exclusion for any loss or expense that P.F. Chang's assumed under contract.

   Federal argued that the data breach did not constitute a "Privacy Injury" because the "Record[s]" compromised were not the records of the company bringing the claims (Bank of America), but rather customer records, and that any liability was assumed by contract.

   P.F. Chang's cited the "reasonable expectation doctrine," which provides any reasonable insured would assume that was coverage in part because of the broad marketing claims of Federal, and that the definition of "Privacy

Injury" does not exclude claims by those other than the person to whom the records belong.

The court sided with Federal.

8. Cyber policies may not provide coverage for intentional acts. In *Travelers Property Cas. Co. of America v. Federal Recover Svs.,* 103 F.Supp.3d 1297 (D. Utah 2015), Global Fitness sued Federal Recovery Services, Inc. ("FRS") and Federal Recovery Acceptance, Inc. ("FRA") dba Paramount Acceptance ("Paramount") (collectively, "Defendants"). The Defendants tendered the defense to their insurer, Travelers.

   The Defendants are in the business of providing processing, storage, transmission, and other handling of electronic data for their customers. Travelers insured the Defendants under a CyberFirst Policy.

   The Defendants entered into an agreement with Global Fitness to process Global's members' financial accounts and transfer member fees to Global. Global later entered into an Asset Purchase Agreement ("APA") with L.A.Fitness. Global informed the Defendants that they would need to return the member accounts data back to Global. The information was not produced. "Rather, FRA withheld the Member Accounts Data until Global Fitness satisfied several vague demands for significant compensation."

   Global filed suit against the Defendants for promissory estoppel, conversation, tortious interference, breach of contract and breach of implied covenant of good faith, and fair dealing. Global asserted that the Defendants "knowingly harmed Global Fitness's rights under the APA with L.A. Fitness."

   Defendants tendered defense of the action to Travelers. Travelers accepted the tender under a full and complete reservation of rights, including the right to seek a judicial declaration as to its right and obligations under the policy.

   The Travelers' policy provided coverage if the loss was caused by an "errors and omissions wrongful act." The policy defined "errors and omissions wrongful act" as "any error, omission, or negligent act."

   The court found that Global's allegations that Defendants knowingly withheld information and refused to turn it over did not sound in negligence. Thus, Travelers had no duty to defend.

9. Cyber coverage may be denied if a contract excludes it. In *Spec's Family Partners Ltd. V. The Hanover Insurance Co.,* 2017 WL 3278060 (S.D.

TX, 2017), the U.S. District Court for the Southern District of Texas found no coverage for about $9.5 million in PCI costs assessed under a merchant services agreement which contained a contract exclusion. While this matter was reversed on appeal by the 5th Circuit Court of Appeals, the court did not find the exclusion inapplicable, but rather held that non-contractual claims had also been asserted.

10. Insurers may deny coverage if the insured fails "to follow minimum required practices," regarding continuously implementing security procedures. In *Columbia Casualty (CNA) v. Cottage Health System,* (2015 WL 2393298 (C.D. Cal.) (Trial Pleading), Cottage suffered a data breach involving about 32,500 confidential medical records. Litigation arose and CNA funded a $4.1 million settlement under a complete reservation of rights. CNA then filed a declaratory judgment action seeking a declaration that it was not obligated to provide Cottage a defense or indemnification. CNA cited an exclusion in its policy for failure to follow minimum security practices. It argued that the breach would not have occurred had Cottage implemented security risk controls that it had represented to CNA that it had in its policy application. Ultimately, Cottage successfully moved to dismiss the action due to Columbia's failure to participate in the mandatory alternative dispute resolution process mandated under the cyber insurance policy. 2015 WL 4497730 (C.D. Cal. July 17, 2015)

11. *Why doesn't a professional policy cover everything?*

    a. Typically a professional policy covers claims arising out of the provision of "professional services."

    b. Most do not contain specific cyber liability exclusions. But, a cyber policy is designed to cover liabilities that do not arise from the provision of "professional services," i.e., from actual legal services. Things typically *not* covered include:

        (1) Fines or penalties
        (2) Loss of revenue from business interruption
        (3) Inadvertent data breaches or losses

12. *What if there is overlapping coverage?*

    a. There often is not overlapping coverage. Insurers are generally loath to cover non-traditional risks, particularly with the proliferation of cyber policies. The insurer may take the position that there was a way for you to secure coverage available, and you are responsible for choosing not to get a cyber policy.

b. Even if there is overlapping coverage, though, you will likely be glad you have the cyber policy. The premiums are typically much lower than a professional policy, so if your cyber policy responds you will not see the big jump in premiums the next year.

c. The retention for the cyber policy would likely be lower.

d. The claims department relative to the cyber policy will likely be more familiar with cyber liability issues and may respond faster.

VI. OTHER COVERAGE CONCERNS

A. Coverage for Cyber-Physical Risks

1. Most cyber policies *exclude* physical bodily injury and property damage to prevent duplicate coverage with general liability policies. But what about bodily injury or property damage that results from a cyber-related peril?

2. The "Internet of Things" is a phrase often used to refer to networked consumer devices. (Buchanan, John, Cho, Dustin, "When Things Get Hacked: Coverage for Cyber-Physical Risks," Insurance Coverage Litigation Committee, American Bar Association, March 3, 2016). The more things are related, the more risk there may be that some will be hacked. Examples include drones, car functions in place now, medical devices, garage doors, home appliances including HVAC, even toys. It is certainly possible that one or more of these will be hacked and result in injury to persons or property.

3. There is a growing concern for insuring medical devices which are vulnerable to cyber attacks. For example, devices such as pacemakers, insulin pumps, patient monitors, and other life-supporting devices may be hacked, infected with malware or accessed by unauthorized users. (Scott Swift, Brian Bassett, and Cheryl Vollweiler, "Is Any Body Safe? Insuring Medical Devices Against Cyber Attacks," *CLM Magazine*, March 2019.)

4. There is also a growing concern for hijacked robots which may cause physical harm. (Anthony Cuthbertson, "Hacked Sex Robots Could Murder People, Security Expert Warns," *Newsweek*, January 1, 2018.)