Chapter 3

Cyber Privacy and Data Protection Law

Remember the first time someone told a secret of yours even after they promised never to tell? That is exactly how it feels to hundreds of millions of people every year when they learn their secrets were betrayed by companies they trusted. Knowing that their private health or financial information is somewhere on the dark web going to the highest bidder causes them untold angst. People hold their privacy dear, and when it becomes violated, they will seek ways to punish those responsible for violating their trust. Despite the existence of many privacy laws prohibiting privacy violations, many companies still violate these laws. Understanding privacy law will enable you to keep customers' secrets and continue to earn their trust.

Privacy in the digital world becomes more complex when you add technology. Facial recognition, identification microchips, voice recognition assistants such as Amazon's Alexa, Google Street View mapping cars equipped with cameras filming every inch of where we live, and big data engines harvesting our every move of digital existence has made protecting privacy rights a whole lot harder.

This chapter will help you to:

- Understand the types and scopes of data privacy laws.
- Know the types of legal actions that can occur as a result of a data breach.
- Gain insight into the actions necessary to avoid negligence claims in a class action lawsuit.
- Realize that data privacy case law set the precedents for determining data breach litigation outcomes.
- Prepare your cybersecurity program in advance to support data breach litigation.

3.1 Common Law of Privacy

Quite often various amendments and laws are cited as the basis for privacy rights; however, most citations tend to be wrong. Did you know, for example, the US Constitution contains no expressed right to privacy? The Bill of Rights does, however, provide some protections of privacy in matters of beliefs, searches, home, etc., but stops short of specifying privacy as a fundamental right. If you remember back nearly 30 years during Judge Robert Bork's Supreme Court confirmation hearing, he stated: "that no such general right of privacy exists." In the absence of clear guidance from the Constitution, we need to look to the law to establish a basis for privacy. This background is essential to your understanding of how privacy rights are legislatively created within the US.

I want to provide a little history in establishing what I believe is an excellent definition of *privacy.* In fact, courts will often refer to this definition of *privacy* even though it was drawn from a court case occurring 60 years ago. In this instance of *Housh v. Peth, privacy* was defined in a way I believe you will agree holds true today:

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 causes mental suffering, shame or humiliation to a person of ordinary sensibilities. *(Housh v. Peth,* 1956)

In the *Housh v. Peth* opinion, you will see the origins of virtually all of today's data privacy laws past and present. The concepts of legitimate concern and wrongful intrusion form the foundation of local, state, and federal data privacy statutes. This *privacy* definition should clarify your mission of ensuring customer privacy.

Sixty-six years before Housh v. Peth outlined privacy, the concern of privacy was raised when in 1890, Samuel Warren and Louis Brandeis wrote in a Hardvard Law Review article titled *The Right to Privacy* that privacy is the "right to be left alone" (Brandesis & Warren, 1890). Their article was written

in response to an emerging technology of the time, photography. We should expect privacy to continue to evolve as technology evolves.

3.2 Privacy Laws

One of a government's principal responsibilities is to protect its citizens, safeguarding them from foreseeable harm. This responsibility to protect extends to cyberspace where lawmakers legislate protection through Internet privacy laws. State and federal governments strive to protect our digital persona or representation by using privacy preserving legislation. Our digital persona is all the private information that describes who we are. These laws extend to virtually every form of digital media and consumer-facing Internet technology. Understanding the legal aspect of privacy law will allow you to make decisions on how you can modify your organization's privacy practices. I encourage you to leverage the *Housh v. Peth* definition to incorporate and align your company's privacy policies.

In the US, no single privacy law exists, and it would not be unusual for you to need to be aware of over 60 pieces of state privacy legislation should you have customers throughout the nation. Add to that various federal and industry regulatory privacy statutes, and that number quickly grows. Enforcement of privacy laws varies. Regulatory agencies may not have the force of law behind them, but they nonetheless have civil financial penalty authority to enforce their privacy regulations. State and federal privacy laws have the force of law behind them, and a negligent or criminal invasion of privacy violation could result in incarceration.

3.2.1 Children's Privacy Laws

We have all grown up knowing that children must be protected, for they lack the ability to protect themselves. We keep them from playing in the street and talking to strangers. Protecting them from the evils of the digital world is no different. According to the Pew Research Center, 88% of all teens (13 - 17 years old) have access to a desktop or laptop computer (Clement, 2018). This creates a potentially large victim pool for Internet-based crimes. We all need to commit to ensuring the privacy rights of children. If your organization interacts with minors digitally, there are specific laws with which you will need to be familiar.

3.2.1.1 Federal Children's Privacy Law

Enacted in 1998 by the US Congress, a groundbreaking privacy law became effective on April 21, 2000. The Children's Online Privacy Protection Act (COPPA) went into effect to restrict information collected on children under the age of 13. The act specifies that website providers must adhere to a privacy policy that requires verifiable consent from a parent or guardian for a child to access their site. The website provider must also document that appropriate safeguards are deployed to ensure the safety and privacy of the children using their site. The act restricts the type of digital marketing toward children.

In 2013, the act was modernized to reflect the increased use of mobile devices and social networking of minors where cookies and geolocation information can be used to track children's location and online activity. If your organization markets to children or allows children access to any of your company's digital media, you must comply with COPPA. A court can fine a website operator who violates COPPA penalties of up to $41,484 per violation.

The following is my summary of the COPPA provisions you would need to follow:

- Conspicuously post a comprehensive privacy policy.
- Directly notify parents of collection and use data gathered.
- Obtain verifiable parental consent.
- Allow parents to review the personal information collected.
- Protect the confidentiality, security, and integrity of children's information.
- Retain personal information for only as long as is necessary.
- Refrain from gathering more information than is reasonably necessary.

> **TIP:** Turn these requirements into a self-assessment checklist to validate that your organization follows COPPA requirements to protect children's privacy.

The act has a safe harbor provision that allows industry groups, companies, or other entities to submit an application for a self-regulatory framework for complying with the act's final rule. You can opt in to one of these safe

harbor provisions to comply with COPPA. A safe harbor provision is a rule within a regulation that specifies that if you adhere to certain rules of conduct, you will be in compliance with an act. If you use one of these frameworks you will be deemed in compliance with COPPA and subsequently exempt from Federal Trade Commission (FTC) enforcement actions. You can still, however, be fined if your practices are found to have willfully violated your chosen self-regulatory safe harbor framework. As of June 2016, the FTC has approved eight safe harbor programs (Federal Trade Commission - COPPA Safe Harbor Program) including:

- Aristotle Age Verification Solution.
- Better Business Bureau's Children's Advertising Review Unit (CARU).
- Entertainment Software Rating Board (ESRB) Kids Seal.
- Privacy Vaults Online Inc. (PRIVO).
- Safe Harbor, Identity, and Consent Service Provider.
- The Internet Keep Safe Coalition (iKeepSafe).
- Samet Privacy (kidSAFE).
- TRUSTe's Children's Privacy Program.

On August 30, 2018, PRIVO launched GDPRkids™ Privacy Assured Program a dedicated program of compliance with the General Data Protection Regulation (GDPR). The program will show your organization's obligations as it relates to protecting children's privacy under GDPR.

The FTC has the authority to issue regulations to enforce COPPA. Curious as to how many companies have been fined over COPPA, I searched the FTC site for "COPPA violations" and was quite surprised over the extent of what I found. Table 3-1 presents some of the largest of the 20+ COPPA enforcement actions to date.

Table 3-1. COPPA Enforcement Actions

Company	Violation	Settlement
Google and YouTube	Collected kids' personal information without parental consent.	$170,000,000
Musical.ly (TikTok)	Failing to obtain parental consent before the collection or use of such information, and failing to delete such personal information following	$5,700,000

	requests from parents.	
Oath, Inc. (AOL)	Tracking online behavioral advertising auctions placing adverts on hundreds of websites that it knew were targeted at children under 13 — such as Roblox.com and Sweetyhigh.com.	$4,700,000
Vtech	Collected information from children without parents' permission through connected toys violating children's privacy.	$650,000
Explore Talent	Collected the same range of personal information from users who indicated they were under age 13 as from other users and made no attempts to provide COPPA-required notice or obtain parental consent before collecting such information.	$235,000
InMobi	Tracked the locations of hundreds of millions of consumers, including children, without their consent, in many cases totally ignoring consumers' express privacy preferences.	$950,000
Yelp	Improperly collected children's information.	$450,000
Tint Co	Encouraged kids to turn over their email addresses, but the company didn't get parental permission.	$300,000
Playdom, Inc. (Disney)	Illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' prior consent.	$3,000,000
Sony BMG Music	Improperly collected, maintained and disclosed personal information from thousands of children under the age of 13, without their parents' consent.	$1,000,000
Xanga.com	Collected, used, and disclosed personal information from children under the age of 13 without first notifying parents and obtaining their consent.	$1,000,000
Mrs. Fields	Failed to obtain verifiable parental consent before collecting personal information from children under 13. In addition, failed to post applicable policies.	$100,000

In September 2016, the New York State Attorney General's (AG) Office closed a two-year investigation dubbed Operation Child Tracker. The AG secured $835,000 in COPPA violation settlements with Hasbro, Mattel ($250,000), Viacom ($500,000) and JumpStart ($85,000). Hasbro was not

fined however, because they participated in the COPPA safe harbor program. The benefit Hasbro enjoyed of participating in a safe harbor act shows the importance of safe harbor acts.

3.2.1.2 State Children's Privacy Laws

Some states do not believe that the federal government's COPPA act goes far enough to protect the children of their state. Subsequently, they have enacted their (own) privacy statutes to protect children. If you operate in California or Delaware or have children as customers there, you will need to be aware of these 2015 laws. California passed the Privacy Rights for California Minors in the Digital World regulation and Delaware passed the Delaware Online Privacy and Protection Act, extending privacy to include removing unwanted information on minors and prohibiting the sale of products known to be harmful to children. More states will adopt these provisions in their existing child privacy laws going forward.

Both states have added four more years to the age their statute applies by defining minors as under the age of 18, as well as prohibit the marketing of products known to be harmful to children (e.g., alcohol, guns, and R-rated materials). The California statute differs from the Delaware law in that it permits minors or parents to remove directly or request the removal of information or photos posted on a website, online service, application (mobile or online), etc. Website or service providers must comply with the removal request. This type of law has been coined in the press as *data erasure law.*

3.2.2 Healthcare Data Privacy Laws

If you have spent any amount of time reviewing the various Health Insurance Portability and Accountability Act's (HIPAA) proposed, interim, and final rules you may have been as confused as I was. Since 1996, there have been numerous amendments to HIPAA, which makes keeping all of them straight challenging at best. This confusion may be one of the reasons so many companies today still find themselves under investigation for HIPAA violations and paying substantial fines.

3.2.2.1 HIPAA Privacy Rule

Much has been written on HIPAA which passed in 1996; however, you have probably heard less about the legal aspect of the Standards for Privacy of Individually Identifiable Health Information, known as the "Privacy Rule." Originally, Congress did not enact privacy legislation in HIPAA, forcing the US Department of Health and Human Services (HHS) to develop a rule regarding privacy. The Privacy Rule was passed on December 28, 2000, with an effective date of April 14, 2001. What is important for you to know is this rule established a set of standards for ensuring the privacy of health information and specifying the manner in which you are allowed to disclose protected health information (PHI). If you are a health care clearinghouse, health plan, or healthcare provider you are considered a covered entity and required to comply with this rule. The rule also specifies the rights your patients have in controlling the use of their PHI.

The enforcement of the Privacy Rule comes under the auspice of the HHS Office for Civil Rights (OCR). Enforcement activities include voluntary compliance oversight and the issuing of financial penalties for noncompliance. The OCR has broad latitude in deciding how to handle violations and can assess penalties up to $50,000 per violation or $1.5 million annually. Published August 14, 2002, the final rule's effective compliance date was October 15, 2002. By now, you are considered in violation of the act if you have not implemented the required privacy controls within your enterprise.

Being equally curious regarding HIPAA violations and fines as I was of COPPA, I set out to the www.hhs.gov website to search for interesting cases. I found that financial penalties for noncompliance can be significant as Maryland-based Cignet Health learned on February 4, 2011, when they became the first company under the act fined for violating its provisions. Cignet's $4.3 million penalty was a result of their violating 41 patients' rights when they denied them requested access to their medical records between September 2008 and October 2009. Remember the act's provision that patients have control over their medical records? This is an example of what happens if you don't provide them with timely access to their records.

Cignet is not the only example of companies paying substantial fines for violating the Privacy Act. Massachusetts General Hospital paid a $1 million penalty in 2011 for a 2009 incident where an employee left PHI of 192

patients on a subway train in Boston. And in case you are thinking these cases of old don't represent what happens today, you would be wrong. Take the recent examples of Feinstein Institute for Medical Research that agreed to pay $3.9 million and undertake substantial remediation of their privacy safeguards on March 17, 2016. On July 16, 2016, the University of Mississippi Medical Center (UMMC) agreed to pay $2.75 million for violating the Privacy Act. The sad tale of all these companies paying fines is that the money could have, and should have, gone toward improving their privacy controls in the first place.

At this point, you may be asking yourself how so many companies can violate a privacy standard that has been in existence for over 16 years. In fact, according to HHS, there have been 213,561 complaints filed under the Privacy Act through July 31, 2019. Of these claims, 27,109 have been investigated and resolved to require covered entities make changes to their privacy practices. The most interesting facts about HHS' data is that 65 cases resulted in fines totaling nearly $102,681,582 and 760 complaints were severe enough to be referred to the Department of Justice (DOJ) for criminal investigation (US Department of Health and Human Services, 2019).

In cases of willful violations, the OCR can refer to the DOJ to pursue criminal charges. The act states that accessing PHI without authorization and subsequently disclosing the information to a third party can result in a jail term of up to 10 years in addition to a maximum fine of $500,000 for disclosures made for personal gain. The first DOJ criminal referral led to a 16-month prison sentence for a former employee of a Seattle, WA cancer clinic who fraudulently obtained credit cards using PHI and charged about $9,000 in a patient's name *(FirstEver HIPAA,* 2004). There have been approximately two dozen convictions to date involving incarceration. The OCR Privacy Rule allows state healthcare protection legislation to trump the OCR's Privacy Rule if their (states) privacy protections are greater than OCR's. One example of this is the Texas Health and Safety Code's protection of health records that includes a broader definition of what is considered a covered entity including some private companies. Table 3-2 shows some of the largest HIPAA fines assessed by the OCR.

Table 3-2. Largest HIPAA Fines

Date	Covered Entity	Fine	Reason
2019	Cottage Health	$3,000,000	Risk analysis failure; Risk management failure; No BAA.
2019	Touchstone Medical Imaging	$3,000,000	Settle breach exposing over 300,000 patients' protected health information.
2018	Anthem	$16,000,000	Cybercriminals had breached its defenses and had gained access to its systems and members' sensitive data. With assistance from cybersecurity firm Mandiant, Anthem determined this was an advanced persistent threat attack - a continuous and targeted cyberattack conducted with the sole purpose of silently stealing sensitive data.
2018	University of Texas MD Anderson Cancer Center	$4,348,000	Impermissible disclosure of ePHI; No Encryption.
2018	Fresenius Medical Care North America	$3,500,000	Risk analysis failures, impermissible disclosure of ePHI; Lack of policies covering electronic devices; Lack of encryption; Insufficient security policies; Insufficient physical safeguards.
2017	Children's Medical Center of Dallas	$3,217,000	A breach of patients' electronic protected health information (ePHI) had occurred. The breach involved the loss of a Blackberry device containing the ePHI of 3,800 patients. The device had not been encrypted and was not protected with a password, allowing any individual who found the device to access the ePHI of patients.
2016	Advocate Health Care Network	$5,500,000	Three data breaches affected the protected information of roughly 4 million people compromises demographic information, clinical information, health insurance information, patient names, addresses, credit card numbers and their expiration dates, and dates of birth.
2016	New York-Presbyterian Hospital	$2,200,000	Television film crews for the show "NY Med" filmed two patients in the hospital without obtaining their authorization. OCR found the hospital also allowed film crews "virtually unfettered access to its healthcare facility, effectively creating an environment where PHI could not be protected from impermissible disclosure to the ABC film crew and staff.
2015	Tripple S Management	$3,500,000	Mailing of a pamphlet that showed the Medicare Health Insurance Claim Numbers of subscribers.

2014	New York-Presbyterian Hospital and Columbia University	$4,800,000	Settle charges from a 2010 breach when a Columbia-based physician attempted to deactivate a personal computer connected to the New York-Presbyterian network that contained patient information.
2014	Concentra Health Services (Addison, Texas)	$1,700,000	An unencrypted laptop was stolen from one of its facilities in 2012.
2013	Oregon Health & Science University	$2,700,000	Two 2013 data breaches affecting more than 7,000 patients total. In the first breach, an unencrypted laptop containing patient information was stolen from a surgeon's vacation home. In the second breach, residents and physicians-in-training had stored patient information in a Google-based cloud system that was not approved for storing such data.
2013	Advocate Health System	$5,550,000	Three data breaches that occurred in 2013. In total, the three incidents compromised the protected health information of 4 million individuals.
2013	WellPoint (Indianapolis)	$1,700,000	Data breach exposed the protected health information of more than 612,000 individuals in a database. The investigation found inadequate policies or safeguards to protect such information.
2012	Alaska Department of Health and Social Services	$1,700,000	Stolen USB hard drive containing protected health information. The OCR's investigation found ADHSS did not have adequate policies and procedures in place to safeguard electronic protected health information.
2011	Cignet Health of Prince George's County	$4,300,000	Failing to cooperate with Office for Civil Rights (OCR) investigations and demonstrating “willful neglect” to comply with the Privacy Rule.
2009	CVS Pharmacy	$2,700,000	Failed to take reasonable and appropriate security measures to protect sensitive information of customers and employees.

3.2.2.1.1 Law Enforcement HIPAA Disclosure

The act does allow a covered entity to disclose limited PHI under certain circumstances to law enforcement in the course of official business. However, it is critical that a fully vetted legally reviewed policy and procedures document is implemented to prevent Privacy Rule violations.

Law enforcement officials do not care about your violating HIPAA when pursuing a case, and your organization will be the one left with the consequences. Table 3-3 provides guidance for the development security policies covering interactions with law enforcement when patient information is requested or demanded.

Table 3-3. Law Enforcement Interaction Security Policy Guidance

Reporting Scenario	Disclosure Examples
Requested reporting	- Specific patient name request - Court order - Victim information - Patient in custody - HIPAA compliant authorization
Mandatory reporting	- DUI testing - Elderly abuse patient - Child abuse patient - Patient injured by a weapon - Deceased patient resulting from a crime
Permitted reporting	- Criminal conduct - Criminal or victim identification - Avert serious or imminent crimes

For more information regarding law enforcement interactions check out HHS' Disclosures for Law Enforcement Purpose information at http://www.hhs.gov/hipaa/for-professionals/faq/disclosures-for-law-enforcement-purposes. You should also create policies in conjunction with your organization's legal counsel.

3.2.2.1.2 HITECH Act

In 2010, the Health Information Technology for Economic and Clinical Health (HITECH) Act was included within the American Recovery and

Did You Know?

Coffey Health System agreed to pay $250,000 to settle allegations that it falsely attested to conducting a security risk analysis as required under the HITECH Act electronic health records financial incentives program. Two whistleblowers in the case - the hospital's former CIO and corporate compliance officer - who filed a lawsuit under the federal False Claims Act - will receive $50,000 of the settlement.

How does your organization monitor for executive fraud?

Source:
https://www.careersinfosecurity.com/hospital-to-pay-250000-after-alleged-false-hitech-claims-a-12569

Reinvestment Act (ARRA). The act was primarily designed to promote the adoption of health information technology during the economic crisis in the US. The act included provisions for ensuring the privacy of electronically transmitted health information. On January 17, 2013, the OCR issued the final rule that requires expanded requirements for privacy. If you are a covered entity, you should have been in compliance with the HITECH Act beginning in September of 2013. Here is what the HITECH Act requires you to comply with:

- **Business Associates (BA).** BAs are now on the hook for complying with certain provisions of HIPAA. BAs can include software providers, service providers, and other companies that provide products or services in the health care industry.
- **Electronic Health Record (EHR) Access.** Companies using EHR must allow access in a timely fashion to patients requesting their records.
- **Enforcement.** The act provides strict enforcements of its provisions consisting of fines up to $1.5 million per year. Willful neglect offenses will be given the highest priority with some cases referred to the DOJ for criminal prosecution. Enforcement is also extended to business associates.
- **Breach Notification.** Covered entities must disclose data breaches of PHI that occurred on unencrypted information. Breaches exceeding 500 records must be reported to HHS, and you will end up on the OCR

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information or more affectionately known in the industry as the wall of shame (US Department of Health and Human Services, n.d.). Affected patients must also be notified.

TIP: Follow the HIPAA Privacy Rule to achieve compliance with the provisions of the HITECH Act.

3.2.2.1.3 HIPAA Breach Notification Rule

The Interim Final Rule dated August 24, 2009 (Breach Notification Rule) added a new subpart D to part 164 of title 45 of the Code of Federal Regulations to implement the Breach Notification provisions established in the HITECH Act. The Breach Notification Rule states that "compromises of security or privacy of the protected health information" means that a disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. An objective risk assessment approach is required to determine the risk that the PHI has been compromised. Table 3-4 is a risk assessment questionnaire I created for a healthcare organization. It may help you in performing a risk assessment to determine the extent of compromised PHI.

Table 3-4. PHI Risk Assessment Questionnaire

No.	Risk Question	Responses
1	Was PHI included in the data breach?	Yes or No
2	How many records were breached?	500+
3	How many PHI identifiers were disclosed?	0 to 18
4	Can the identifiers disclosed lead to discovering the patient?	Yes or No
5	Did an unauthorized person access the PHI?	Yes or No
6	Was the PHI viewed or acquired?	Viewed or Acquired
7	Was the PHI encrypted?	Yes or No

This approach is more comprehensive than the four-factor approach suggested by HIPAA. If you want a full scope risk assessment program, the National Institute of Standards and Technology (NIST) offers a comprehensive HIPAA Security Rule Toolkit. Go to https://scap.nist.gov/hipaa/ to download a free copy of the Toolkit.

3.2.2.2 Veterans Benefits, Health Care, and Information Technology Act

In 2006 S.3421, the Veterans Benefits, Health Care, and Information Technology Act, requires the Department of Veterans Affairs (VA) to implement agency-wide security and privacy procedures to protect sensitive personal information (SPI) of employees and patients. This act was passed following the 2006 data breach of over 26 million veterans when a VA employee's computer was stolen from home.

The act requires that in the event of a data breach of SPI processed or maintained by the VA, the VA's Inspector General must conduct an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of SPI. Based upon the risk analysis, if the Secretary of Veterans Affairs determines that a reasonable risk exists of the potential misuse of SPI, the Secretary must provide:

- Credit protection services.
- Identity theft insurance.
- Notification to affected patients and employees.
- A report detailing the findings of the independent risk analysis for each data breach.
- A report of compromised sensitive personnel records issued to the US Department of Defense (DOD) Armed Services Committee.
- Liquidated damages paid by contractors who caused the data breach.

What is quite different about this act is the requirement for liquidated damages if your company was found to be the cause of the data breach. In this context, a contractor is considered in breach of contract for not protecting SPI and must pay a predetermined sum to compensate the VA for the damage caused. This would include the cost of credit monitoring services, notifications costs, etc. More information about the provisions of

this bill can be found at https://www.congress.gov/bill/109th-congress/senate-bill/3421.

3.2.3 Federal Privacy Laws

Today a framework of robust federal laws covers the protection of personal information. Some of these statutes are very specialized in their scope, while some have broad reaching protections for personal information. The first federal law was published in 1970; since then, by my count, 22 other data privacy laws have passed.

In Table 3-5, the federal statutes, acts, and regulations directly or indirectly apply to ensuring the privacy of information or prohibiting invasions of privacy.

Table 3-5. Federal Statutes Related to Privacy

Year	Bill	Title	Description
1970	H.R.15073	Fair Credit Reporting Act (FCRA)	Protection of personal information related to credit reporting.
1974	513 of P.L. 93-380	Family Educational Rights and Privacy Act (FERPA)	Restricts the disclosure of educational records.
1974	S.3418	Privacy Act	Code of privacy practices for federally held information.
1978	H.R.4727	Privacy Protection for Rape Victims Act	Protection of rape victim identities.
1978	H.R.14279	Right to Financial Privacy https://www.congress.gov/bill/95th-congress/house-bill/14279	Privacy of customer financial records from government scrutiny.
1984	S.66	Cable Communications Policy Act (CCPA)	Personally identifiable information (PII) must be destroyed once no longer necessary.

1986	H.R.4952	Electronic Communications Privacy Act (ECPA)	Privacy of electronic data transmission by computer.
1986	18 US Code Chapter 121	Stored Wire and Electronic Communications and Transactional Records Access - Stored Communications Act (SCA)	Protects stored electronic communications that are configured to be private.
1988	S.496	Computer Matching and Privacy Protection Act	Privacy principles for government information sharing.
1988	S.2361	Video Privacy Protection Act (VPPA)	Prohibits disclosure of PII by video service providers.
1991	S.1462	Telephone Consumer Protection Act (TCPA)	Protection of subscriber privacy rights.
1994	H.R.3355	Driver's Privacy Protection Act (DPPA)	Limits the disclosures of PII in records maintained by state departments of motor vehicles.
1994	H.R.2243	Federal Trade Commission Act (FTCA)	Privacy protections for children and consumer information.
1996	H.R.3103	Health Insurance Portability and Accountability Act (HIPAA)	Privacy of personal health information (PHI).
1998	16 CFR Part 312	Children's Online Privacy Protection Act (COPPA)	Protection of minors' privacy.
1999	S.900	Gramm-Leach-Bliley-Act (GLBA)	Protection of non-public personal information (NPI).
2003	H.R.2622	Fair and Accurate Credit Transactions Act (FACTA)	Protection of credit card information to prevent identity theft.
2003	S.877	CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act)	Prevents invasion of individual privacy through the issuance of spam.
2006	H.R.4709	Telephone Records and Privacy Protection Act (TRPPA)	Prohibits pretexting to obtain personal phone records.
2009	H.R.1	American Recovery and Reinvestment Act -	Data breach notification of PHI.

		Health Information Technology for Economic and Clinical Health Act (HITECH Act)	
2010	S.2092	Fair Debt Collection Practices Act	Prevents invasion of individual privacy.
2013	45 CFR Parts 160 and 164	HIPAA Breach Notification Rule	Notification and penalties for violations of PII.
2013	H.R. 6671	Video Privacy Protection Act Amendments Act of 2012	Allows PII to be disclosed with informed, written consent of the consumer.
2015	H.R.1428	Judicial Redress Act	Allows European citizens to sue for unlawful PII disclosures.
2015	H.R.22	FAST Act - Driver Privacy Act	Limitations on data retrieval from vehicle event data recorders.

It is important to note that many of these laws could have amendments since their first passage. For each applicable statute, ensure that you are referencing the most current version by accessing the link provided or searching for the law or act at https://www.congress.gov/.

TIP: Create a spreadsheet of the laws mentioned in this chapter that apply to your organization and include hyperlinks to their sources. Identify the privacy requirements of each law and map those to your organization's privacy policies, practices, and controls.

3.2.4 Cybercrime on Tribal Lands

Did You Know?
History has shown that casinos have been attractive targets for hackers as evidenced by cyberattacks at The Hard Rock Hotel and Casino, River Cree Resort and Casino and the Sands Corporation.

When you consider that 56 million acres or a little over 92,000 square miles of land are held in trust by the U.S. government for various Native American tribes (U.S. Department of the Interior, 2019) it is not inconceivable to think that cybercrime could occur somewhere in an area approximately the size of the state of Idaho. There are nearly 575 federally recognized American Indian Tribes in the U.S. and the FBI is responsible for investigating cybercrimes that occur on the nearly 200 Indian reservations that violate federal law. No small feat when you consider the over 450 gambling operations run by 240 tribes represent a significant technology footprint.

For cybercrimes that don't break Federal law, jurisdiction becomes somewhat ambiguous. In 1978, the Supreme Court case Oliphant v. Suquamish stripped tribes of the right to arrest and prosecute non-Indians who commit crimes on Indian land. If both victim and perpetrator are non-Indian, a county or state officer must make the arrest. If the perpetrator is non-Indian and the victim an enrolled member, only a federally certified agent has that right. If the opposite is true, a tribal officer can make the arrest, but the case still goes to federal court.

Even if both parties are tribal members, a U.S. attorney often assumes the case, since tribal courts lack the authority to sentence defendants to more than three years in prison. The harshest enforcement tool a tribal officer can legally wield over a non-Indian is a traffic ticket. The result has been a jurisdictional tangle that often makes prosecuting crimes committed in Indian Country prohibitively difficult (Crane-Murdoch, 2013).

3.2.4.1 Sovereign Immunity of Data Breach Laws

There has yet to be a data breach at a tribal casino or tribal business to test the concept of sovereign immunity against a third party claim or class-action lawsuit. But this depends on what state the casino is located. Some states have negotiated gaming compacts stating that sovereign immunity could be waived for tort claims. An example of this is found in Harold McNeal et ux. v. Navajo Nation et al., case number 18-894, in the Supreme Court of the United States. In this case U.S. District Judge Martha Vazquez ruled that the Navajo Nation had waived sovereign immunity to the McNeals' state court lawsuit when its council ratified the tribe's 2003 gaming compact with New Mexico. Judge Vazquez rejected the tribe's contention that its council lacked

the authority to send tort suits to state court, and the tribe subsequently appealed to the U.S. Tenth Circuit Court. This precedent could prove instrumental in a data breach class-action lawsuit.

3.2.4.2 National Indian Gaming Commission

The Indian Gaming Regulatory Act was enacted by the United States Congress on October 17, 1988, to regulate the conduct of gaming on Indian Lands. IGRA establishes the National Indian Gaming Commission and the regulatory structure for Indian gaming in the United States. Public Law 100-497-Oct. 17, 1988 100th Congress Sec. 2701.

Casino owners should at a minimum leverage the National Indian Gaming Commission no-cost IT vulnerability assessment testing for tribes and tribal regulators, which provides a tribal gaming facility with a complete vulnerability analysis of their IT system. Showing due diligence and what a reasonable person would do begins with demonstrating that minimum security requirements are followed through use of the IT vulnerability assessment tool.

3.2.5 State Privacy Laws

Every state in the US has at least one privacy law that seeks to protect their citizens from invasions of privacy and theft of PII. California is one such example of a state having many laws. Presently, California has six individual privacy laws covering constitutional rights, health information, online privacy, and other privacy protections. It is not unusual for large organizations to comply with 50 to 60 different state privacy laws, making this extremely confusing. Big companies have chief privacy officers (CPO) to address the multitude of privacy laws. To make this situation even more complicated is that depending on the situation, a state or federal privacy statute can preempt one another. You will need to understand the hierarchy of these laws to ensure you are focusing your efforts correctly. To help you understand the areas state privacy laws focus on, Table 3-6 provides the most common identification attributes you should be protecting.

Table 3-6. Common Records Covered State Privacy Laws

Record Category	Record Type
Personal identification	- Name - Address - Driver's license - Employment - Passport - Phone number - Photo (minors) - Email - Medical - School records - Social Security numbers
Financial identification	- Bank - Credit card - Insurance - Loan - Tax - Utility bills
Government identification	- Arrest records (non-public) - Military ID - Court documents (non-public) - Polygraph results - Wiretaps

3.2.6 State Chief Information Privacy Officer (CIPO) Laws

Several states have passed laws that require the establishment of an Office of Privacy and Data Protection and/or hire a Chief Privacy Officer. These states recognize that passing data privacy laws alone without having a privacy Czar at the helm is a band aid approach to protecting the privacy right of their state citizens. Table 3-7 shows some of the states that have passed specific CPIO laws.

Table 3-7. State CIPO Laws

State	Statute	Main Provisions
Arkansas	HOUSE BILL 1793	• Create position of CPO • Oversee, develop, and implement state privacy program

Ohio	Ohio Rev. Code § 125.18(B)(6)	• Employ CPO • Annual privacy impacts statements
Massachusetts	Mass. Gen. Laws Ch. 7D, § 4B (2018 H.B. 3731)	• Appoint CIPO • Privacy Ombudsperson
Washington	RCWs > Title 43 > Chapter 43.105 > Section 43.105.369	• Create office of privacy and data protection • Appoint CPO

There are other states, counties and even cities that have hired CPOs. For example, the cities of New York and Seattle as well as the counties of Maricopa, Maui, and San Diego have all hired CPOs in the past several years.

3.2.7 International Privacy Laws

More than 90 countries have passed data privacy laws. From Angola to Zimbabwe, these laws vary in scope and complexity. Penalties range from fines to incarceration and in some cases such as China, Nigeria, Saudi Arabia and Pakistan, even death. The growth in data protection and privacy laws as well as their rapid rate of enhancements can quickly become a compliance nightmare for a cybersecurity or privacy manager. The Asia Pacific region is experiencing the greatest number of new laws, and European countries tend to have the most mature and comprehensive laws.

If your organization is a multi-national concern, then you may already be breaking data privacy laws and don't even know it. Unless you have created a detailed compliance program that maps each country of operation to the privacy provisions of each law considering data collection, storage, processing, transmission, etc., you cannot know if you are compliant or not. You must also consider transborder data privacy provisions considering the legal implications of data in the cloud. For most of us, we don't have the resources to keep track of all these international data privacy laws. I can highly recommend that you review DLA Piper's *Data Protection Laws of the World* handbook (DLA Piper).

3.2.7.1 China's No Place to Hide Law

On December 1, 2019, China's Cybersecurity Multi-Level Protection Scheme (MLPS 2.0) became law. Dubbed by many as the "Nowhere to Hide" law, MLPS requires encryption backdoors for any encryption algorithms used in China. MLPS is in fact a comprehensive data gathering and surveillance system. Ministry of Public Security and other internet security agencies of the PRC government and the CCP will have the encryption backdoors to do as they see appropriate for their respective security programs. Any organization conducting business in China should already know that the government monitors and captures Internet traffic. MLPS just puts a name on what many have already suspected.

MLPS sets out the technical and organizational controls all companies in China must follow to comply with MLPS-related Internet security obligations mandated by China's Cybersecurity Law. All companies and individuals must abide by the following three standards:

- GB/T 22239 - 2019 Information Security Technology - Baseline for Multi-level Protection Scheme
- GB/T 25070 - 2019 Information Security Technology - Technical Requirements of Security Design for Multi-level Protection Scheme.
- GB/T 28448 - 2019 Information Security Technology - Evaluation Requirements for Multi-level Protection Scheme.

No English version of these standards are presently available, so you must be careful of the source of any translations that are sure to emerge.

One of the most significant aspects of this law is that no technology that blocks access by the Ministry of Public Security is permitted. No VPN, no encryption, no private servers. You also must recognize that the China Ministry of Public Security is required to install back doors or other message/data interception devices or systems to achieve full access. You will need to assume that China Telecom and Chinese based ISPs are required to comply (Sussman, 2019).

Sussman, Bruce. (2019, October 15). *Chilling Assessment of China's New Cybersecurity Law: 'There Is No Place to Hide.'* SecureWorld. Retrieved from https://www.secureworldexpo.com/industry-news/what-does-new-china-cybersecurity-law-do

3.3 Data Breach Laws

The term *data breach* seems to garner more fear than *data privacy* and subsequently the lion's share of press. I believe this is due more to the impression that a violation of privacy is more about revealing embarrassing information and a breach of data is associated more with financial impacts. According to a recent Verizon data breach report, there were over 41,686 security incidents across 180 countries and territories, of which 2,013 were confirmed cases where confidential information was exposed making this by all measure a serious issue that you must address (Verizon, 2019). When you begin viewing the various data privacy and data breach laws, you will realize a fine line exists between the two types of laws. The important point is that data breach laws predominately deal with the issue of disclosure. Data breach laws follow a similar framework consisting of compliance, triggers, safe harbor, notification, remedies, and penalties.

3.3.1 State Data Breach Laws

Did You Know?
In the past ten years California, New York, Texas, Florida, Georgia and Oregon accounted for top states with the most reported data breaches. Since 2008, 9,696 data breaches occurred across the U.S. involving more than 10.7 billion records.

Source:
https://www.fastcompany.com/90366574/which-states-had-most-data-breaches-california-and-new-york

All 50 states, District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach laws. Only the Northern Marianas Islands and American Samoa have not enacted data breach legislation (National Conference of State Legislatures, 2019b). The common denominator of these statutes is their specification of PII. If an entity were to intentionally or accidentally disclose PII, the offending entity would be required to make a public notification as well as pay a financial penalty.

In reviewing data breach laws, I noticed six common characteristics:

1. **Type of Personal Information.** Personally identifiable information consists of Social Security numbers, driver's license numbers, account numbers, credit or debit card numbers, phone numbers, addresses, health information, and other depending on the state.
2. **Harm Standard.** Notification is not required if, after an investigation, the breached company determines that no reasonable likelihood of harm occurred to customers.
3. **Data Format.** Laws can cover electronic, paper, or both types of records, as well as consider whether the data was encrypted or unencrypted.
4. **Notification Requirement.** Upon the confirmation of a breach, the company has an obligation to report to one of more organizations consisting of consumer reporting agencies (e.g., Experian, Equifax, or TransUnion), a state's Office of the Attorney General, and the FTC.
5. **Notice Period.** Ten business days to 30 to 45 or up to 60 calendar days.
6. **Form of Notification.** Notification methods vary by state consisting of mailed written notice, electronic (email), telephone, or fax.

The first thing you will need to understand about data breach notifications is the safe harbor provision, meaning that if your data is encrypted, then no notification would be required. That is unless it is in Tennessee. In July 2016, Tennessee became the first state to require breach notification even if the data is encrypted (Embry, 2016).

3.3.2 Federal Data Breach Laws

The federal government had not specifically addressed data breach or breach notification in a singular law until the introduction of H.R.1770 - the Data Security and Breach Notification Act of 2015. This bill is designed to protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide notice in the event of a breach of security. This bill would result in a law that would differ from other data breach notifications in that a *national* public notification would be required. The bill was introduced and approved by the committee for further consideration in April of 2015. From that point forward it has been stalled because of discussion over limitations in scope and the

preempting of states with existing laws. Many state legislators see this as a duplicate law to their state notification laws. Other industry groups, agencies, and states have voiced concerns over the fact the proposed act applies only to breaches that can be directly linked to identity theft or financial fraud. The FTC would be the enforcement agency for this bill if it becomes law. In 2017 it was placed on the Union Calendar, which is a separate calendar used by the House of Representatives for bills requiring money. I am still not sure if this bill will ultimately make it, but it still lives.

Another bill, H.R.1704 - the Personal Data Notification and Protection Act, was introduced in March of 2015 to address certain businesses that use, access, transmit, store, dispose of, or collect sensitive, personally identifiable information. An interesting aspect of this bill is that it categorizes reporting requirements by data breach size, with levels of 5,000, 10,000, and 500,000 in any 12-month period. The Department of Homeland Security (DHS) would be the agency to report data breaches. A form of safe harbor is also included in this bill. The FTC would be the enforcement agency for this bill should it become law.

I am not convinced either of these bills will become law, at least as they are currently drafted. You should watch these laws as the momentum on Capitol Hill is poised to make progress in passing a national data breach law by the 116th congressional session, 2019-2020, in light of the media attention data breaches have garnered.

In case you are asking yourself, “What about the HIPAA and Gramm-Leach-Bliley (GLBA) Acts? Don’t they have data breach provisions?” Yes, they do; however, they are specific to health care and financial industries respectively. I discussed HIPAA breach notification previously, which leaves GLBA. GLBA breaches of consumer financial data are guided by the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice issued by bank regulatory agencies pursuant to GLBA. The guidance requires that a financial institution notify affected customers “as soon as possible” if the institution determines that misuse of “sensitive customer information” has occurred or is reasonably possible (Federal Deposit Insurance Corporation, 2005).

3.3.2.1 Gramm-Leach-Bliley Act (GLBA)

Did You Know?

On February 27, 2018, the FTC announced a settlement for Venmo's violations of the GLBA privacy and safeguards rules. Specifically, the FTC alleged that Venmo misled consumers regarding privacy and the extent to which consumers' financial accounts were secured. Venmo is required to obtain biennial third-party assessments of its compliance with these rules for 10 years.

Does your organization comply with the provisions of GLBA?

Source:
https://www.huntonprivacyblog.com/2018/03/02/ftc-announces-settlement-for-venmos-alleged-violations-of-the-glbas-privacy-and-safeguards-rules/

Financial Modernization Act of 1999 or GLBA regulates the collection, use, disclosure as well as protection of personal information by financial institutions. This Federal law, effective May 23, 2003 requires financial institutions to explain how they share and protect their customers' private information. Remember every year you get a rash of privacy notification in the mail? Well you have GLBA to thank for that. GLBA defines financial institutions as banks, credit unions, insurance companies, securities firms; also debt collectors, real estate appraisers, check cashing businesses and mortgage brokers. Some retailers and automobile dealers that extend or arrange credit or issue credit cards are also on the list.

One of the provisions of GLBA is to provide customers with a notice of privacy practices. GLBA covers nonpublic information that is defined as any personally identifiable information that you would provide to obtain a financial product or service. The most important aspect of GLBA are the privacy and safeguard rules require:

- **314.3 Standards for Safeguarding Customer Information**

  (a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are

appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Ensure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

- **314.4 Elements**

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage,

transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

Violating GLBA brings sizable penalties for non-compliance including imprisonment for up to five years and fines up to $100,000 for each violation; officers and directors can also be fined up to $10,000 for each violation.

3.3.2.2 Red Flags Rule

In 2003, Congress amended the Fair Credit Reporting Act (“FCRA”) to require the Federal Trade Commission (“FTC”) and certain other federal agencies (together, the “Agencies”) to jointly adopt identity theft red flags rules and guidelines. At that time, FCRA did not require or authorize the Securities and Exchange Commission (“SEC”) or Commodity Futures Trading Commission (“CFTC”) to adopt these rules. Instead, the FTC had

authority to adopt and enforce these rules with respect to SEC- and CFTC-regulated entities. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 amended FCRA to transfer identity theft rulemaking responsibility and enforcement authority to the SEC and CFTC with respect to the SEC- and CFTC-regulated entities.

The FTC developed a series of markers, or "red flags," to help organizations detect fraud attempts before criminals can make any actual progress. These markers became ensconced within SEC Regulation S-ID (17 CFR 248, Subpart C) or the FTC Identity Theft Red Flag Rule. The penalty for non-compliance with the Red Flags Rule is $3,500 maximum in civil fines per violation and up to $2,500 per infraction due to the FTC.

The SEC's identity theft red flags rules require certain SEC-regulated entities to adopt a written identity theft program that includes policies and procedures designed to:

- Identify relevant types of identity theft red flags;
- Detect the occurrence of those red flags;
- Respond appropriately to the detected red flags; and
- Periodically update the identity theft program.

The SEC's identity theft red flags rules apply to SEC-regulated entities that qualify as financial institutions or creditors under FCRA and require those financial institutions and creditors that maintain covered accounts to adopt identity theft programs. SEC-regulated entities that are likely to qualify as financial institutions or creditors and maintain covered accounts include most registered brokers, dealers, and investment companies, and some registered investment advisers.

3.3.2.3 Federal Government Security Memorandum

If you work for the federal government, you will need to be aware of the 2007 memorandum for the heads of executive departments and agencies titled, Safeguarding Against the Breach of Personally Identifiable Information. The memorandum states, "Safeguarding personally identifiable information in the possession of the government and preventing its breach

are essential to ensure the government retains the trust of the American public" (Johnson, 2007). Agencies are required to:

- Develop and implement a breach notification policy.
- Use encryption to protect PII.
- Develop incident response plans.
- Limit access to authorized personnel.
- Create external breach notification protocols.

3.3.3 International Data Breach Laws

The United Nations (UN) tracks 160 countries with respect to their efforts in protecting information. Figure 3-1 provides a breakdown of the legislation status relating to data protection for the 160 countries tracked by the UN.

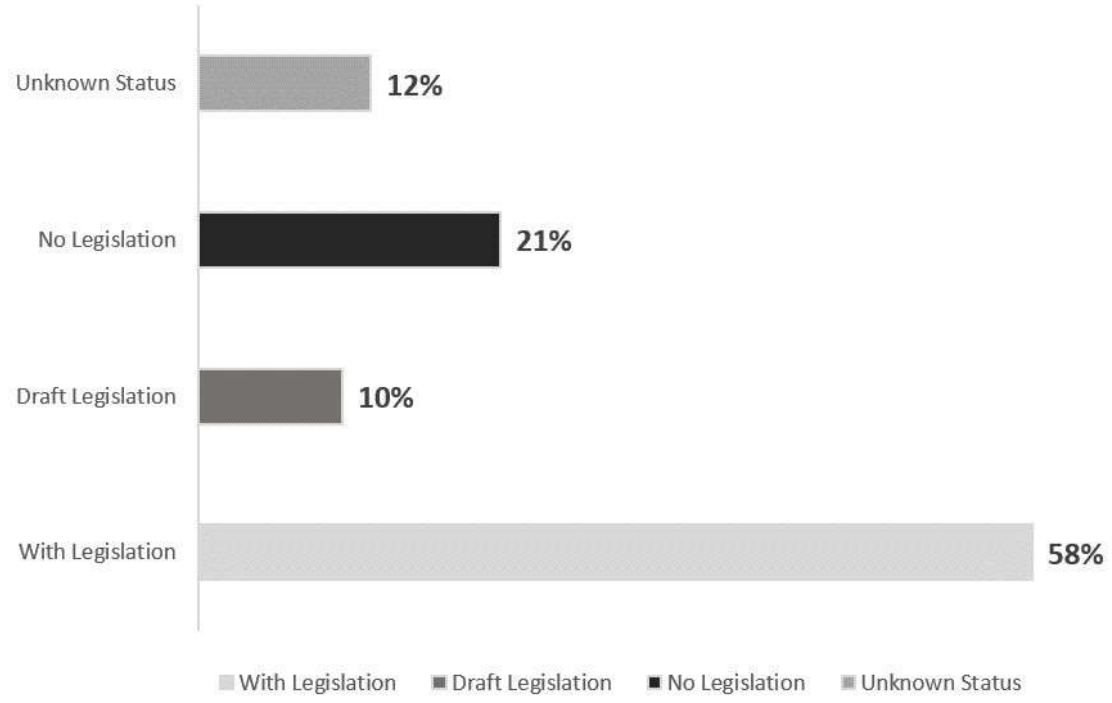

Figure 3-1. International Data Breach Law Status

The DLA Piper's *Data Protection Laws of the World* handbook provides a view of data breach laws of over 110 countries (DLA Piper, 2019). You can access the book and select the *breach notification* tab to investigate these laws for the countries applicable to your organization.

I know most of you won't have the time to download and read this handbook, so I have taken the liberty to outline the privacy laws of the G7 in Table 3-8. The G7, short for the Group of Seven is an international economic organization consisting of the seven largest International Monetary Fund (IMF) advanced economies in the world: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.

Table 3-8. G7 Privacy Laws

Country	Privacy Act	Bill	Date
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	36th Parliament, Bill C-6	April 13, 2000
France	Data Protection Act	Ordinance 2018-1125	December 12, 2018
Germany	Federal Data Protection Act (FDPA)	Bundesdatenschutzgesetz (BDSG)	July 5, 2017
Italy	Italian Privacy Code	Legislative Decree No. 196/2003	August 10, 2018
Japan	Act on Protection of Personal Information (APPI)	Act No. 57	September 7, 2018
United Kingdom	Data Protection Act 2018	2018 c. 12	May 23, 2018
United States	No Single Data Protection Act	Not Applicable	Not Applicable

It won't take you long to notice that the US is the only one of the G7 that does not have a unified national data protection act. The US has a patchwork quilt of privacy laws as identified in Table 3-5. You will no doubt also notice that many of the national data protection acts of the G7 occurred on or around the date of the adoption of the GDPR. The move of these G7 countries to harmonize their existing national data protection laws with the GDPR was critical to eliminate confusion in compliance and enforcement.

3.3.3.1 New and Emerging International Privacy Laws

This book does not allow covering all the international laws nor does it make sense to duplicate the work already completed in DLA's excellent handbook. But I do want to highlight recent changes in international privacy law that could impact those reading this book with international business models. Some of these laws even have ramifications for organizations who have customers in the following countries but no physical presence.

- **Australia -** The Privacy Amendment (Notifiable Data Breaches) to Australia's Privacy Act came into effect in February 2018. Organizations with an annual turnover of over 3 million AUD will have to disclose data breaches that pose a "real threat of serious harm" within 30 days of their discovery or faces fines of up to 1.8 million AUD.
- **Brazil -** In 2020, the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018 will take effect. This law is very similar to the GDPR especially in its expanded definition of territory. Companies with customers in Brazil will need to comply with their law in the event of a data breach even though they have no physical operations located within their country.
- **Bahrain -** This country is the first Middle East country to enact a comprehensive data protection law. Law No. 30 of 2018 - Personal Data Protection Law became effective August 2019 and includes fines of up to BD 20,000 (US $53,200) or imprisonment for up to one year.
- **China -** China has a confusing landscape of data privacy with more than 200 laws, rules, and national standards in varying degrees of standing from proposed to enact as law. In an effort to simplify all these privacy rules, in March 2018, China's National Information Security Standardization Technical Committee (TC260) issued a national standard, the Personal Information Security Specification, which covers the collection, storage, use, sharing, transfer, and disclosure of personal information. TC260 is China's version of our National Institute of Standard and Technology.

  China is stepping up their efforts to reduce or eliminate the misuse of private data. In May of 2019, China further codified its protection of information by releasing a new data protection law. This new data protection law requires labeling of data feeds user receive that are

driven by their personal data. Internet service provided are also required to delete collected data if users choose to turn off recommendations and ads. China's data privacy laws only apply to Chinese territories. Taiwan maintains it on Personal Data Protection Law (PDPL) law that was last revised in 2015.

- **India -** Specific rights of consumers and requirements for technical safeguards regarding the processing of personal data, including cross-border data transfers are expected to be in India's comprehensive Personal Data Protection Bill introduced in 2018. Ratification is expected sometime in 2019.
- **Peru -** The Protection of Personal Data outlined in Peru's Personal Data Protection N° 29733 (PDPL) law was amended in 2018 and includes a unique stipulation in that it prohibits marketing texts and emails to anyone without prior informed consent.
- **Thailand -** Thailand's Personal Data Protection Act (PDPA) went into effect in May of 2019. The PDPA is like the GDPR in several ways, including the broad definition of personal data, the requirement to establish a legal basis for collection and use of personal data, extraterritorial applicability, and potentially harsh penalties for non-compliance.

We just need to go down the alphabet to identify other countries such as Indonesia, New Zealand, Kenya and Zimbabwe to identify those planning on introducing new data privacy and protection acts. 2019 - 2020 looks to be a watershed year for new or enhanced international data privacy laws.

3.3.4 General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) was approved by the EU parliament on April 14, 2016 and became effective May 2018. The GDPR replaces the EU Data Protection Directive and is designed to:

- Standardize disparate data privacy laws throughout Europe.
- Protect EU citizen privacy.
- Harmonize EU data protection and privacy safeguards.
- Encourage compliance through meaningful fines and sanctions.
- Put EU citizens back in charge of their personal data.

GDPR applies to organizations located within the EU as well as organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, the EU data subjects. GDPR applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location. Figure 3-1 provides a model of how GDPR is designed.

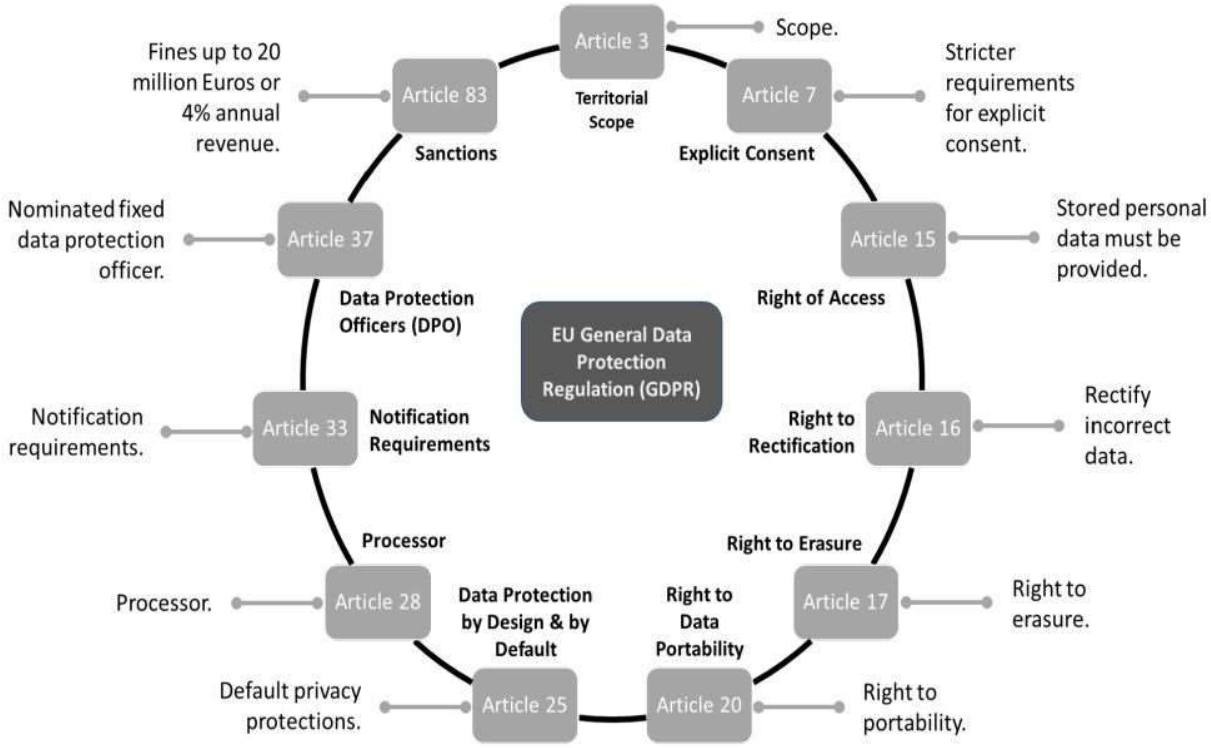

Figure 3-1. EU GDPR Model.

The GDPR differs from the EU Data Protection Directive in the following ways:

- **Directive vs. Regulation -** GDPR carries more clout and removes the discretionary language that comes with a directive. The GDPR applies to all member states of the EU and removes data protection inconsistencies of member states.
- **Jurisdiction Expansion -** The coverage of GDPR is expanded past European boundaries and extends compliance to any organization that houses or processes EU citizen information regardless of location.
- **Citizen Consent and Rights -** Organizations can no longer use ambiguous terminology or confusing legalese to define or secure

consent. Organizations must clearly define the terms of consent and how data will be used in plain language. Citizens also have the right to access (right to access) and receive (data portability) their own data as well as have it erased (right to be forgotten) on demand.

- **Privacy Safeguards -** Privacy is now a legal requirement where privacy protection must be designed in systems and processes to meet the requirements of GDPR.
- **Enforcement -** The GDPR is similarly enforced through courts, with penal and administrative sanctions in addition to civil remedies. What has changed is the amount of the fines a court can levy for a violation. Fines can go as high as EUR 20 million or four percent of an organization's turnover or annual sales.
- **Breach Notifications -** Under GDPR it is no longer necessary to submit breach notifications to each local privacy authority. A Data Protection Officer (DPO), which is a mandatory appointment would make the notification to a single and relevant authority.

2019 is the year when GDPR enforcement ramped up. I believe that for every data breach experienced here in the US, a parallel GDPR enforcement in cases EU citizens are impacted will be launched. Table 3-9 provides a summary of the some of the initial fines levied under GDPR.

Table 3-9. Largest GDPR Fines

Date	Covered Entity	Country	Fine (US)	Reason
2019	Google	France	$55,000,000	Lack of transparency, inadequate information and lack of valid consent regarding ads personalisation.
2019	Active Insurance	France	$198,702	Online check revealed that the accounts of the company's customers were accessible via hypertext links referenced on a search engine.
2019	Unicredit Bank	Romania	$143,507	Failure to apply appropriate technical and organizational measures, both in the determination of the processing means and the processing operations themselves, to effectively implement data protection principles.

2019	Sergic	France	$441,559	Users could access documents from other individuals on the site by modifying a URL.
2019	Haga Hospital	The Netherlands	$507,793	Lax controls over logging and access to patient records. In one instance, 197 employees accessed one Dutch celebrity's medical records.
2019	MisterTango UAB - Payment Processor	Lithuania	$67,889.80	Accidentally exposed a website with a list of consumer payments and payment details, including personal information.
2019	Bisnode	Poland	$242,858	Scraped 7.6 million contacts from public registries, such as the Polish Central Electronic Register and Information on Economic Activity.
2018	Centro Hospitalar Barreiro Montijo	Portugal	$441,559	Hospital had 985 registered doctor profiles while only having 296 doctors. Moreover, doctors had unrestricted access to all patient files, regardless of the doctor's specialty.

The companies fined above are just the beginning with U.K. Data Protection Authority the Information Commissioner's Office announcing in July of 2019 intends to fine British Airways and Marriott International for violating the GDPR $228 million and $124 million respectively in July 2019 (Davies, 2019).

> **TIP:** Create a GDPR impact statement based on four percent of your organization's annual turnover as well as covert EUR $20 million to determine total fine exposure.

GDPR compliance still requires work world-wide. A report by Thompson Reuters released approximately one year to the day that GDPR took affect states that:

- More companies are failing to meet global data privacy regulations.
- Many companies have found GDPR compliance more difficult than expected.
- Half of companies are at risk of falling further behind.
- An increasing number of companies have now been subject to enforcement actions.

- Companies are becoming less open and pro-active with consumers.
- Board and C-suite concern and engagement on data privacy issues is falling.
- GDPR is now consuming a greater proportion of data privacy budgets (Thomson Reuters, 2019).

3.4 Data Breach Litigation

The frequency and scope of privacy data breaches are increasing substantially. Yahool's September 2016 announcement of the theft of one-half billion customer records when hackers breached their systems in 2014 set a high bar for data breaches. Yahoo! became aware of the cyberattack only when Yahoo! customer information went up for sale on the dark web, two years after the attack. Three months later, in December 2016, Yahoo! revealed that another earlier hack in 2013 affected more than one billion accounts.

The important point about the Yahoo! hack and other examples is that injuries to the plaintiff don't necessarily need to be immediate. Many data breach lawsuits suffer dismissal from lack of standing. However, some cases are avoiding dismissal by proving future injury. Courts have decidedly taken two approaches to data breach lawsuits, specifically class action lawsuits. On the one hand, courts have ruled in some cases that plaintiffs who cannot show actual injury or cannot prove they made a purchasing decision based on the defendant's privacy policy have no standing to claim injury. On the other hand, some courts have ruled that injury does not have to be immediate. The Yahoo! data breach case may change some court's position regarding the issue of future harm.

3.4.1 Injury vs. No-Injury Class Action Lawsuits

From July to October 2013, hackers stole 350,000 instances of credit card data from Neiman Marcus Group, LLC (Neiman). The data compromise came to light when some of Neiman's customers noticed fraudulent charges on their credit cards in December of that year. Ultimately, 9,200 credit cards would be fraudulently used. In January, Neiman made a public disclosure of the cyberattack. Shortly afterward, several class action lawsuits were filed. These were all consolidated into a single action filed by Hilary Remijas who filed a lawsuit on her behalf and all others similarly situated (class action). The complaint or lawsuit seeking $5 million accused Neiman of negligence, breach of implied contract, unjust enrichment, invasion of privacy, and violation of multiple state data breach laws. Citing the rules of civil

procedure, Neiman moved to dismiss the lawsuit for lack of standing. The judge held that even though credit cards were fraudulently used, the fact that customers were reimbursed proved no financial loss or harm had occurred. A district court dismissed the case based on the fact the plaintiffs lacked standing or a demonstrable harm. The case was appealed, argued, and decided between January and July 2015. It is the result of this appeal that makes data breach law interesting.

In a first of its kind legal precedent, the US Court of Appeals for the Seventh Circuit in Chicago, IL found that the Neiman plaintiffs in a data breach case satisfactorily identified harm, even though no harm had occurred. The judge ruled that the plaintiffs proved some particularized, concrete, and redressable injuries as a result of a data breach and that Neiman caused the injury. Subsequently, this court reversed the original court's decision allowing the case to go forward.

The plaintiff claimed injury based on lost time and money resolving the fraudulent charges and efforts protecting themselves from future identity theft. They also claimed financial loss of buying items at the store that they would not have, had they known of the cyber breach and lost control over the value of the personal information.

Three things are required to prove standing: *injury-in-fact, causation,* and *redressability.* The *injury-in-fact* requirement was satisfied by the claims that resolving fraudulent charges and protecting oneself against future identity theft were injurious. For causation, the court relied on the Target Corporation data breach case as a precedent and wrote that when Neiman argued that other data breaches could have caused the plaintiffs' card compromises, the burden of proof shifted to the defendant to prove they did not cause it. The fact that Neiman admitted the cyber breach and notified all their customers they were at risk and had customer credit cards fraudulently used was enough to prove *causation.* To meet the requirement of *redress* (compensation), the plaintiffs claimed that injury would come from future expenses for mitigation cost and damages. The court agreed *(Remijas v. Neiman Marcus Group, LLC,* 2015).

> **TIP:** Ensure that you carefully write the breach notification letter as well as any public disclosure statements in a manner that does not admit liability

> or determine harm that could be used against your company in a court of law.

The US Court of Appeals for the Seventh Circuit's ruling goes against a 2013 US Supreme Court decision that states that an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action, and redressable by a favorable ruling" *(Clapper v. Amnesty Int'l USA).* The Neiman case may have a significant impact on future privacy violation lawsuits where defendants have been able to have class action lawsuits readily dismissed for lack of standing. In fact, it had already been cited in 2016 in *Lewert v. P.F. Chang's China Bistro, Inc.* Here the Seventh District Court overruled a lower court's decision on standing citing its previous *Remijas v. Neiman Marcus Group, LLC* ruling. Further complicating the outlook of how courts will rule in data breach cases is a second US Supreme Court decision in May 2016 in the case of *Spokeo v. Robins.* Here the US Supreme Court vacated (overruled) the US Ninth Circuit Court's ruling approving the class action lawsuit stating that concrete harm could not be abstract but needed to be tangible and that *injury-in-fact* was not proved. Here the court ruled that a plaintiff cannot allege only a statutory violation but must also show actual injury as a result of the offense to sue in federal court.

If you find that your company is named in a data privacy breach litigation, your ability to guide your business using the three requirements of standing will significantly aid your legal defense. Guiding the legal defense requires that you work with your legal department primarily in the area of causation to attempt to prove other factors could have been involved in your customer's alleged injury. Would you be able to show that your data collection, processing, and security practices would hold up to scrutiny in a court of law?

3.4.2 Data Privacy and the US Supreme Court

In July 2014, the US Supreme Court made its strongest case for digital privacy when it ruled (Riley v. California) the search of a cell phone for incriminating information in a murder case was unconstitutional. In this case, the court unanimously agreed that electronic devices carry many forms of sensitive and private information that trigger privacy protections. The

court's ruling treats these types of data-holding devices like an extension of a person's home allowing Fourth Amendment protection. I expect that as more cases make their way to the US Supreme Court, further elaboration of digital privacy rights will be enumerated.

Three landmark US Supreme Court opinions, described below, may shape how your company would defend itself in a privacy lawsuit.

3.4.2.1 City of Ontario, California, et al. v. Quon

On June 17, 2010, the US Supreme Court ruled that employers have the right to access and search employee messages under reasonable circumstances. In this case, a City of Ontario, CA SWAT team member (officer Quan) used his city-provided pager to send and receive sexually explicit messages to his wife and mistress. Officer Quan believed that he had an expectation of privacy because his supervisor stated he could use his pager for personal messaging if he reimbursed the city. The sexting on his city-issued communication device became apparent in 2002 when an audit of officer texting overages was analyzed to determine if the increase was due to personal texting that would subsequently cost the city more money for a different texting plan. The city requested and was provided with transcripts of officer Quan's text messages from the service provider Arch Wireless. The matter was turned over to internal affairs where only working time personal messages were reviewed. It was found the majority were during working hours and subsequently officer Quan was disciplined.

Quan and several other city employees brought suit claiming their Fourth Amendment rights, as well as the Stored Communications Act (SCA), was violated. The court ruled that the city had a legitimate right to audit officer Quan's texting records, and thus his Fourth Amendment rights were not violated. The amendment guarantees a person's privacy and security from invasive and arbitrary government actions. In this case, the city's actions were neither invasive nor arbitrary. Also, before acquiring the pagers, the city published a computer usage, Internet, and email policy that allowed the city to monitor and log all email and Internet use. The policy, however, did not cover wireless network text messaging. This would have been a critical mistake if it had not been for the fact the city verbally and in written form stated that text messages would be considered as email under the policy. The

SCA violation naming Arch Wireless as a defendant was viewed as not relevant and was dropped.

What is important to note from the US Supreme Court opinion is the statement, .employer policies concerning communications will, of course, shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." For you as a manager, you will need to ensure that cybersecurity policies support the rule of law, are clearly communicated, often reminded, only modified in writing, and revised to include new technologies.

This opinion shows that you will need to ensure that searches of employee data are done for legitimate business purposes and that employees are aware of their obligations under your company's cybersecurity policy.

3.4.2.2 Campbell-Ewald Co. v. Gomez

On January 20, 2016, the US Supreme Court held that an unaccepted offer settlement under Rule 68 of the Federal Rules of Civil Procedure (settlement offer) without more, cannot moot (nullify) a named plaintiff's claim. The term *without more* in this context means just an offer of a financial settlement. In this case, Gomez received unsolicited text messages and filed a putative nationwide class action lawsuit against the Campbell Ewald Company seeking treble (triple) damages alleging willful violations of the Telephone Consumer Protection Act (TCP A). Before the deadline to file for class action certification expired, Campbell made a settlement offer providing Gomez full relief on his TCPA claim. Gomez allowed the offer to expire after 14 days under the Rule 68. Campbell then moved to dismiss the case. That motion was dismissed; however, the lower court granted a summary judgment motion for Campbell on a separate sovereign immunity issue.

Sovereign immunity is where the government cannot be sued, and in this case, Campbell was working under a government contract and therefore enjoyed the protection of sovereign immunity. Campbell's sovereign immunity motion would ultimately be overturned by a higher court. The case was argued before the US Supreme Court, which wrote the opinion that when a settlement offer is not accepted, "the parties remain adverse; both

retained the same stake in the litigation they had at the outset." The court also ruled that "a federal contractor is not entitled to immunity from suit for its violation of the Telephone Consumer Protection Act when it violated both federal law and the government's explicit instructions." *(Campbell-EwaldCo. v. Gomez,* 2015).

The result of this opinion is that companies will find it difficult to "buy off" the primary plaintiff to avoid a class action lawsuit or hide behind sovereign immunity while working on government contracts.

3.4.2.3 Tyson Foods, Inc. v. Bouaphakeo

On March 22, 2016, the US Supreme Court ruled that class action plaintiffs may use sampling to establish injury among the plaintiffs. Although not a data privacy case, the court's decision could have wide-reaching effect in data privacy class action lawsuits. In this case, the plaintiffs used an expert study to show the average amount of time required to don and doff protective equipment to claim overtime pay. The court ruled that this data could be used to establish the injury of loss of income to all plaintiffs because it was also admissible to show the employer's liability. The result is that the door is now open for data breach class action plaintiffs to introduce expert studies and statistical models to show how all plaintiffs would be harmed by a data breach.

TIP: If your company is named in a class action data breach lawsuit, you need the knowledge and skills to perform your risk assessment and statistical modeling to calculate the harm or injury to your customers.

Did You Know?

On January 4, 2019 the Yahoo! data breach-related derivative suit was settled for $29 million. The derivative complaint asserted claims against Yahoo's board for breach of fiduciary duty, insider trading, unjust enrichment, and waste.

How would your company deal with a lawsuit brought by a shareholder on behalf of your company?

Source:
https://www.dandodiary.com/2019/01/

articles/cyber-liability/yahoo-data-breach-related-derivative-suit-settled-29-million/

3.4.3 Shareholder Derivative Lawsuits

Nothing strikes fear in a CEO or a board of directors faster than the phrase "shareholder derivative lawsuit." A derivative lawsuit is a lawsuit brought by a shareholder of a corporation on its behalf to enforce or defend a legal right or claim that the corporation has failed to do. When a shareholder feels that management has not done enough to rectify a situation, the shareholder can sue the company to force itself to sue itself. The directors, management, and in some cases other shareholders of the corporation can be named for failing a duty of care. This type of lawsuit is brought when it is deemed the officers and board of directors have ignored an issue, which in the context of our topic is a serious breach of security.

A growing number of derivative lawsuits targeting officers and directors have been filed alleging claims of breach of fiduciary duty by not ensuring their company's cybersecurity program was adequate or challenging their conduct following a breach. Some of the more publicly visible derivative lawsuits involved Target Corporation, TJX Companies, and Wyndham Worldwide Corporation (Wyndham). One of your roles following a data breach should be ensuring the board acts responsibly by providing them with accurate, timely information about what happened. This may be difficult as they may see you as the contributing factor to the breach. You will also need to watch for the passage of the H.R.5069, the Cybersecurity Systems and Risks Reporting Act, as boards of directors may be hiring their own cybersecurity expert to advise them during times of cyberattacks and resulting lawsuits leaving you out in the cyber cold.

The actions of a board leading up to and after a cyberattack will be evaluated to determine their duty of care and whether they acted in the best interests of their company and shareholders. Take, for example, the 2014 lawsuit of *Palkon v. Holmes,* the first case of a decision in a derivative lawsuit resulting from a data breach. Wyndham suffered three data breaches over a three-year period beginning in 2008 resulting in 600,000 compromised customer records. In this case, Dennis Palkon, a shareholder of Wyndham, sent two demand letters to the board requesting they investigate the breach and sue

the employees involved. A demand letter is a letter stating a legal claim which makes a demand for restitution or performance of some obligation. The board considered both letters and responded that it would not be in the company's best interest to do so. Now that Palkon has met the threshold of bringing a derivative lawsuit (issue of demand letters), he filed suit in the US District Court of New Jersey to force the directors to sue their company. The suit named board member Stephen Holmes and nine other Wyndham directors for breach of fiduciary duty, unjust enrichment, and a waste of corporate assets. Unjust enrichment is a claim where defendants believe that directors and officers received bonuses, or the value of their stock increased, through the act of expense reductions by not investing in cybersecurity safeguards.

The case was dismissed without merit; however, valuable lessons can be gleaned from how the board acted during the breaches. These actions proved to the court that they (board) had acted in a fiduciary manner. Their efforts included discussing the cyberattacks and the company's security capabilities during 14 quarterly meetings during the period of the breaches. The board appointed an audit committee to investigate the breaches. The committee met 16 times and regularly reported back to the board. And finally, the company hired a computer forensics company and technology company to implement cybersecurity program enhancements. The board was also actively involved in the previously filed FTC lawsuit against Wyndham for failures in their cybersecurity program. The actions the board took were anything, but gross negligence claimed by Palkon. This case underscores the critical importance of a board involving themselves in a company's cybersecurity program. The board did have a bit of luck in their case - the derivative lawsuit was filed after the board had acquired three years of a security breach and cyberattack experience. Most such suits are filed immediately not giving a board much time to prepare.

> **TIP:** As someone involved directly with your company's cybersecurity program, you may be personally sued in a derivative lawsuit, meaning the company could be forced to sue you for the failure of duty or negligence in a data breach. Ultimately, a personal lawsuit could end up costing tens of thousands of dollars in attorney's fees. You should discuss with your management how your breach-

related legal expenses would be handled in such a scenario.

3.4.4 Securities Fraud Lawsuits

Before the notion of filing derivative lawsuits, parties would file a securities-fraud lawsuit citing various portions of the Securities Exchange Act of 1934 relating to fiduciary responsibility. This was the preferred method of shareholders to challenge directors and officers following a data breach because it had been successfully used over the years to connect lack of management oversite to a breach of security. Two of the largest cases to date include Heartland Payment Systems, Inc. and ChoicePoint, Inc. (now known as LexisNexis Risk Solutions). In both cases, the plaintiff alleged the defendants falsely reported their security controls capability in their 10K statements.

Although both cases were dismissed, they show that securities fraud can be used to sue an organization resulting in significant costs and preoccupation of key employees to defend against the litigation.

If you were not already just a little bit concerned about being part of a data breach lawsuit, then by now you should be on the brink of being cautiously paranoid. Understanding the numerous and varied data privacy laws that apply to your organization’s cybersecurity program should give you an appreciation for the magnitude of work that remains for your cybersecurity program to reach and stay compliant with the dynamic and rapidly changing cybersecurity privacy legislative landscape.

3.5 Privacy Notice Law

Have you ever wondered about all those privacy notifications that seem to all arrive about the same time every year? You can thank GLBA for that, since it is the principal law requiring many companies that have consumers to provide an annual update of their privacy policy regarding their information sharing practices (Federal Trade Commission, 2002). You will need to ask yourself if your company's privacy policy provided to consumers each year is clear and accurate as well as easy to locate. GLBA's main provisions consist of:

- Financial privacy rule, which affords you the control over how your private information is shared among affiliates.
- Pretexting provisions, which aim to stop third parties from acquiring your personal information through false pretenses.
- Safeguard rule, a requirement to establish and maintain safeguards to protect your private information.

Privacy notices apply whenever a company collects nonpublic personal information. How your company gathers and discloses information about consumers is highly regulated by GLBA. If you collect nonpublic personal information directly from the consumer or populate applications with personal information gathered from another source, such as a credit bureau, all the information must be protected by your company. Penalties for violating GLBA can include $100,000 fines for each violation, fines up to $10,000 for each director, and imprisonment up to five years. There are also provisions to double penalties if it is determined that a pattern of illegal activity exists.

Did You Know?

Mignon Hofmann, a former information security officer at San Francisco State, filed a $1 million lawsuit claiming that she was fired by the university in order to sweep a 2014 hack involving significant exposure of student records "under the rug." The student records that were involved in the breach included both financial records and password reset functions.

How well could your company defend a whistleblower lawsuit?

Source:
https://www.bamlawca.com/california-labor-laws/alleged-hack-fired-employee-sues-sf-state-for-1m

3.6 Personal Liability

As a result of numerous data breaches, with senior management lawyering their way out of responsibility, aggrieved parities have begun to search for others to blame outside of a company's board of directors. Shareholders and plaintiffs are turning their attention increasingly toward chief information officers (CIO) and chief information security officers (CISO). In 2015, the CIO of the US Office of Personnel Management (OPM), Donna Seymour, was personally named in a $1 billion lawsuit by the American Federation of Government Employees citing her negligence in securing nearly 22 million current and former employee and contractor records.

This was the second breach to occur on her watch. This lawsuit was poised to set some concerning precedents for CIOs and CISOs alike. Over the next three years the lawsuit was dismissed as well as reinstated when in June of 2019 the U.S. Court of Appeals for the D.C. Circuit largely sided with two federal employee unions in their lawsuit citing the plaintiffs have standing and the lawsuit can continue (Katz, 2019). All correspondence related to cybersecurity sent by CIOs and CISOs is open for discovery and will be analyzed to determine the duty of care claims.

TIP: CIOs and CISOs should send any security assessment reports and correspondence to in-house legal counsel to preserve client-attorney privilege ensuring these types of reports are not available for discovery motions. A file transfer protocol (FTP) server or document management solution can also be used to submit sensitive documents to the legal department to preserve client-attorney privilege.

Did You Know?

In Spec's Family Partners, Ltd. v Hanover Insurance Co., No. 1720263, 2018 U.S. App. LEXIS 17246 (5th Cir. June 25, 2018), the court of appeals found that a contractual liability exclusion in a management liability policy did not excuse the insurer of its duty to defend its policyholder, a private company, against a claim arising out of a payment card data breach.

Does your company's insurance policy provide adequate coverage for executives?

Source:
https://policyholderinformer.com/2018/08/02/seeking-insurance-coverage-for-data-breach-claims-a-recent-case-confirms-that-certain-do-policies-potentially-provide-coverage/

3.6.1 Directors and Officers Insurance

If anyone has ever told you that titles don't matter, well, here is a case in which they do. Directors and officers (D&O) insurance protects the officers and directors, including board members, against allegations of wrongdoing. It protects them against liabilities not already indemnified by the corporation. Companies have this type of insurance because officers and directors can make mistakes and may be personally liable for those mistakes.

D&O insurance just may be the time that titles matter. Having the title of security manager rather than chief information security officer may make all the difference in your being covered under the blanket protections of your company's D&O policy. D&O insurance protects actions of directors, officers, and board members against lawsuits based on failures in employment practices, reporting errors, decisions exceeding authority, and failure to comply with regulations and laws among others. However, D&O policies do not cover any acts of fraud or other types of intentional criminal offenses.

Of importance to you are the protections for failure to comply with regulations or laws. In the event your company is sued for negligence in security controls, will you be covered, and your personal assets protected? D&O policies can vary widely; so it is important that you sit with your business's insurance risk manager and have a discussion of whether the D&O policy covers you. If not, it may also be time to ask for that raise and change in title!

3.6.2 Preemptive Liability Protection

If you feel that your company is not taking your advice to improve cybersecurity and has made public statements overstating its security capabilities, you could take the whistleblower route to mitigate your liability exposure.

For example, in August 2013, LifeLock Inc.'s former CISO, Michael Peters, filed whistleblower complaints with the FTC, Securities and Exchange Commission, and the US Department of Labor for LifeLock's failure to comply with a previous 2010 FTC order to improve security controls. Although it took nearly four years, the FTC filed a motion for contempt against LifeLock, alleging failure to have a comprehensive security program, making false claims about security customers, failing to meet the 2010 recordkeeping requirements, and other claims. LifeLock offered a $20 million settlement that was rejected by the FTC.

In 2015, LifeLock settled with the FTC for a little over $100 million. In reaching the final settlement, LifeLock claimed it had complied with the previous order by achieving certification under the Payment Card Industry Data Security Standard (PCI DSS), a proprietary information security standard. LifeLock's CISO's report on the inadequacies of their security controls was enough to convince the FTC that the LifeLock's PCI DSS certification was insufficient to prove the company acted reasonably. The FTC did not need much convincing as several previous enforcement actions over data breaches occurred to companies who also held PCI certifications. In fact, other data breach examples I cite in this book such as Neiman Marcus and Target were all PCI compliant.

Several months after Peters filed the whistleblower complaint, he was terminated by LifeLock, prompting him to file a complaint against his former company in March 2014 for violating the whistleblower provisions of the Sarbanes-Oxley Act and Dodd-Frank Act by terminating his employment. Peters, as LifeLock's CISO, performed an initial risk assessment and determined that his company's auditing, event logging, incident response, security awareness, security monitoring, and vulnerability testing were far less than the minimum requirements of accepted security practices required by the 2010 FTC order (Ross, 2014). Peters subsequently reached an out of court settlement, and the whistleblower case was dismissed in November 2015.

3.6.3 Cybersecurity Whistleblower Protections

Cybersecurity whistleblowers have both legal and financial reward incentives to go public with evidence of company misdeeds that lead to data breaches. However, the laws don't directly provide protection, but rather protect against retaliation. A subtle, but important point when it comes to defending against a wrongful termination suit. The facts of the case can influence a whistleblower's standing. For example, did the whistleblower violate confidentiality, steal evidence, fail to properly report, etc. The following are some of the laws that provide protections against whistleblower retaliation:

- Dodd-Frank Act.
- False Claims Act.
- Financial Institutions Reform Recovery Act.
- National Defense Authorization Act.
- Sarbanes-Oxley Act.
- Whistleblower Protection Act.

Here are some examples of cybersecurity-related whistleblower settlements:

- **July, 2019 -** Cisco Systems, Inc. agreed to $8 million settlement to resolve allegations it knowingly sold vulnerable video surveillance software to federal, state and local government agencies, exposing government systems to the risk of unauthorized access and the manipulation of vital information. (Constantine Cannon, 2019a)
- **April, 2019 -** IT supplier Fortinet agreed to pay more than $500,000 to resolve a False Claims Act (FCA) case brought by a whistleblower alleging that it routinely supplied the government with products made in China and then doctored the products' labels to make it appear that they complied with the federal Trade Agreements Act. In announcing the settlement, the government emphasized that it was "committed to combatting procurement fraud and cyber risk within U.S. Department of Defense programs." (Constantine Cannon, 2019b).
- **June, 2017 -** Electronic health records (EHR) vendor eClinicalWorks agreed to pay $155 million to resolve claims that it misrepresented the capabilities of its software to fraudulently obtain certification required for government payment. While not involving security standards, EHR

fraud cases demonstrate the government's interest in pursuing vendors for misrepresenting software capabilities. (Constantine Cannon, 2019c).

- **November, 2015 -** NetCracker Technology Corp., which provided telecommunications network support to the Department of Defense, agreed to pay $11.4 million to settle claims that it used employees without security clearances to perform contract work that it knew required clearances. (Constantine Cannon, 2015).

3.7 Data Disposal Laws

If you thought that complying with data privacy and data breach laws would be enough, think again. Your responsibility for protecting the privacy of your customers' data continues until the data makes it to the grave - in this case, the end of life and ultimate disposal of information. Thirty-five states and Puerto Rico have passed laws governing the destruction and disposal of data (National Conference of State Legislatures, 2019a). This aspect of the data lifecycle is so critical that the FTC has even published a rule on how consumer report information should be disposed (Federal Trade Commission, 2005a). On June 1, 2005, the Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule went into effect requiring you to take appropriate measures to dispose of sensitive information derived from consumers (Federal Trade Commission, 2005b).

Take time to review your data lifecycle policy and practices to trace each stop your data makes along the lifecycle to verify that proper privacy protections are implemented including the proper disposal, erasing, or permanent elimination of data no longer required. Table 3-10 is the data compliance lifecycle I developed that has served me well. You may find it useful in tracing your data through your organization.

Table 3-10. Data Compliance Lifecycle

Stage	Summary
Data creation	Prevent data alteration during creation.
Data use	Prevent data misuse and handling when used.
Data transmission	Prevent data interception and alteration.
Data processing	Prevent data alteration when transformed by processing.
Data storage	Prevent theft, destruction, or errors when backed up.
Data archival	Prevent theft, destruction, loss, or errors when archived.

Data disposal	Prevent reconstitution; ensure total destruction.

3.8 Electronic Wiretap Laws

Have you ever wondered if monitoring employee email, website activities, or running surveillance with data loss prevention (DLP) products on employee communications was violating any privacy laws? Well it just may be violating the Electronic Communications Privacy Act (ECPA) if you have not made the proper disclosures. First and foremost, you must ensure that a policy exists and clearly states that your company reserves the right to monitor any digital, audio, or video data sent over company communication lines and networks. Employees need to understand that there should be no expectation of privacy. If you are monitoring data and communications relating to customers, it can be done only if there is a legitimate business need, such as quality assurance, and you have their consent.

The ECPA provides for fines and imprisonment of up to five years for violations unless you adhere to the following:

- **One-Party Consent.** The ECPA does not prohibit interception of communications if either the sender or the recipient gives prior consent. However, consent cannot be implied and must be given prior to the interception.
- **Business Use Exception.** The ECPA does not prohibit interception if it is conducted within the ordinary course of an employer's business and the employer has a legal interest in the subject matter of the conversation.

> **TIP:** If your company has a bring-your-own-device (BYOD) policy, employees, guests, or contractors need to acknowledge that any courtesy communications provided while they are onsite using their own devices may be monitored as well.

This is an area where you are highly encouraged to meet with your legal department to review and approve employee monitoring policies.

3.9 Digital Assistant Privacy Issues

So, there is a joke that starts off “If Alexa, Cortana, Siri and Holly go into a bar who can keep a secret?” The punch line is “none of them.” If you’re wondering who Holly is, it’s the default female name for Google’s digital assistant. These devices constantly record information whether it’s wanted or not. Privacy protections built into these devices are questionable at best and could be used in a court of law if subpoenaed. In January 2017, a New Hampshire judge ordered Amazon to release recordings from an Echo device from a house where two women were found dead. In 2015, prosecutors in Bentonville, Arkansas sought to gain information from an Amazon Echo device as well. In both cases Amazon argued that the requests violated the First and Fourth Amendments. In both cases, Amazon vigorously fought to suppress the requests for Alexa recording.

Extending First (free speech) and Fourth Amendment (unreasonable search and seizure) rights to artificial intelligence has proponents on both sides of the issue arguing the merits for and against. Ultimately, I feel these issues will end up in the U.S. Supreme to be decided.

3.10 Social Media Privacy

If you're like me, you have at least one social media account. Many of you reading this book will have Facebook and LinkedIn at the very least. What some of you may not know, is that more than just our friends and family can see what we post. Companies have sophisticated social media monitoring software that will scan the Internet looking for your social media impressions. Things you said ten years ago could come back to haunt you in a job search. Some companies even require you to turn over your social media usernames and passwords so they can review your background. This is generally seen as an invasion pf privacy and some states are seeking to prevent companies from forcing you to turnover your social media credentials. Table 3-11 shows which states are actively looking to adopt social media privacy laws.

Table 3-11. Social Media Laws

State	Legislation	Status	Provisions
Florida	H.B.493	Pending	Prohibits an employer from requesting or requiring access to a social media account of an employee or prospective employee, prohibits an employer from taking retaliatory personnel action.
Hawaii	H.B. 6	Pending	Adopts uniform laws on protecting the online accounts of employees, unpaid interns, applicants, students, and prospective students from employers and educational institutions.
Massachusetts	H.B 1628	Pending	Social media consumer privacy protection.
Minnesota	H.B.1196	Pending	Protects applicant's and employee's personal usernames and passwords from access by employers, provides for civil enforcement.
New York	A.B. 935	Pending	Uniform Employee and Student Online Privacy Protection Act, relates to the protection of employee and student online accounts.

To date, the states of Delaware (H.B. 109), Illinois (H.B. 4999), Montana (H.B. 343), Nebraska (L.B. 821), Virginia (H.B. 20181) have passed social media privacy laws. There are however three time as many states that have failed their legislative attempts to pass similar laws. To keep up with state activity in passing social media laws checkout http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

3.11 Event Data Recorder (EDR) Privacy

Most of us are unaware that event data recorders have been part of many cars since the mid 1990's. In fact, EDRs were used in 64 percent of all new model cars in 2005. Fast-forward to today and nearly every car has an EDR. EDRs collect a tremendous amount of data including:

- Air bag status
- Braking
- Child restraints
- Crash event duration
- Crash force
- Crashes
- Electronics status
- Engine RPM
- GPS data
- Occupants in car
- Roll angle
- Seatbelt use
- Speed
- Start/stops
- Steering wheel angle
- Tire pressure
- Vehicle speed

When looking at how your car can spy on you it doesn't take long to arrive at the fact that if you're in a crash, your car can basically testify against you in a court of law or your insurance company. To prevent abuses of EDR privacy several states have passed EDR privacy laws. Table 3-11 shows a sampling of states with prohibitions on EDR use.

Table 3-11. EDR Privacy Laws

State	Statute	Prohibition of Data Use
Arkansas	Ark. Code § 23-112-107	Permission cannot be a condition of payment/ settlement of an insurance claim, or of a lease or insurance agreement.

Connecticut	CGS § 14-164aa	Data may not be destroyed or altered after a crash until after a reasonable period to allow law enforcement to obtain a warrant.
Delaware	Del. Code § 3918	Applies to private passenger vehicle insurance issued to individual policyholders.
New Jersey	N.J. Stat. § 39:10B-7 to -9	Prohibits altering or deleting data on a recording device, or knowingly destroying a recording device with the intent to prevent access to or destroy the recorded data within two years after a crash event that resulted in bodily injury or death.
Oregon	Ore. Rev. Stat. §§ 105.925 to .948	Permission cannot be a condition of payment/settlement of an insurance claim, or of a lease or insurance agreement.
Utah	Utah Code § 41-1a-1501 to -1504	Provides that event data recorded on an event data recorder is private and is the personal information of the motor vehicle's owner.
Virginia	Va. Code § 38.2-2212(C)(s), § 38.2-2213.1, § 46.2-1088.6, § 46.2-1532.2	Insurer cannot refuse to renew an insurance policy solely based in the owner's refusal to share data Insurer cannot adjust rates due solely on the refusal to share data.
Washington	Wash. Code § 46.35.010, .020, .030, .040, .050	Requires vehicle manufacturers to ensure that a tool is commercially available and capable of accessing and retrieving data in an EDR.

There are nearly 20 states that have or are about to pass EDR privacy laws. EDRs record information locally to the car, but many also provide a function to upload data to a cloud-based storage device. With hundreds of thousands of automotive accidents and tens of thousands of deaths, law enforcement investigators, prosecutors, and insurance companies want access to these EDRS to prove what happened. The 2015 Driver Privacy Act declared that EDR is the property of the owner or lessee of the vehicle.

The 2015 legislation provides that EDR data may be accessed by a person other than the owner or lessee under five circumstances:

1. Court or administrative order.
2. Consent of the owner or lessee.

3. Investigation of a motor vehicle accident by the Secretary of the Treasury or the National Transportation Safety Board, provided personally identifiable information is not disclosed.
4. Emergency medical response to a vehicle crash.
5. Traffic safety research provided personally identifiable information is not disclosed.

Courts have gone both for an against the privacy argument and whether extracting EDR data violates a person's Fourth Amendment Rights when it comes to requiring a search warrant. Table 3-12 provides a summary on two court rulings involving EDR.

Table 3-12. EDR Judicial Rulings

Case	Ruling
State v. Worsham, 227 So.3d 602 (Fla. Dist, Ct. App. 2017)	**For Defendant:** Reasonable expectation of privacy in the information retained by an event data recorder and downloading that information without a warrant from an impounded car in the absence of exigent circumstances violated the Fourth Amendment.
People v. Diaz, 153 Cal.Rptr.3d 90 (Cal. App. 4th 2013)	**Against Defendant:** Specific data obtained from the SDM was the vehicle's speed and braking immediately before the impact. We agree that a person has no reasonable expectation of privacy in speed on a public highway because speed may readily be observed and measured through, for example, radar devices.

TIP: If your organization provides employee cars, pool transportation or other form of vehicle fleet, ensure the privacy policy covers EDR data access and use.